10. NETWORKS AND THE INTERNET

"Networks and the Internet" Module allows the user to get information and familiarize with a very up-to-date domain: that of computers networks (and maintaining them in good function condition). This Module consists of all the important concepts related to this matter, as well as all the notions necessary for efficiently using networks and their maintenance. The Module also contains theoretical and practical elements meant for guiding the user in acknowledging the computer networks. For those interested in more detailed information, there is a special In depth-analysis chapter emphasizing the whole functioning process of a network: OSI model.
After attending the whole module, the user will be able to use without any problems the computer networks (and even to administrate a small network), thus becoming an efficient user of the Internet.

10.1. Fundamentals of Networks

10.1.1. What is a computer network?

10.1.2. Computer network classification

10.1.3. Local computer networks (LAN)

10.1.4. Wide area computer networks (WAN)

10.1.5. Calculation equipment within a network

10.1.6. Network accounts

10.1.7. Resources' distribution within a local network

10.1.8. Messages within a network

10.2. Calculation Equipment Distributed Within a Network

10.2.1. The server

10.2.2. Categories of servers

10.2.3. Server operating systems

10.2.4. Work stations (Customers)

10.2.5. Operating systems for work stations

10.2.6. Transmission circumstances

10.2.7 Characteristics of the transmission means

10.2.8 Co-axial cable

10.2.9 Twisted Pair cable (TP)

10.7.4. The protocol for files trivial transfer (TFTP)

10.7.5. The protocol for e-mal (Simple Mail Transfer Protocol - SMTP)

10.7.6. The protocol for controlling the transmission (Transmission Control Protocol - TCP)

10.7.7. User Diatagram Protocol – UDP

10.7.8. Internet protocol (Internet Protocol - IP)

10.1. Fundamentals of Networks

In order to efficiently use a work station within a computer network, the user should know the fundamentals regarding networks. For this purpose, the basic compounds of a computers network are detailed and the main categories of computer networks are marked out and thoroughly described. Each compound is described in connection with the others for a better understanding of its purpose and place within a local or wide area network. After attending this section, the user will be able to define a network and its component parts, and will also be able to describe the way it functions.

10.1.1. What is a computer network?

The network is the most important component of the modern technology. Without a (local) network it would be impossible to use chats, Internet, mobile phones or even cable TV.

A computer network consists of a series of calculation equipment that can jointly distribute hardware and software resources.

A computer network consists of a hardware part (servers, work stations, cables, printers and so on) and a software part (as operating systems and applications).

Even though the user has never used before a PC within a network he still has experience in this field. All actual technologies work on network concept basis, regardless to they being connected to computers. The local GSM operator local uses a network that is based on "cells through which the information is communicated and, even though such network is different from a computer network, it is based on the same principles.

Each time you dial a phone number you use an network using amazing priorities. By pressing few buttons, you connect your phone to any phone no matter where this phone is. Due to this remarkable ability, the result seems to the user very natural.

Have you ever thought of the implications of a phone conversation between Bucharest and Naples?

Such process is more complex than it might seem. Automatic systems in the telephone exchange in Bucharest must connect to your line and the inter-city service to transmit your message to the telephone exchange in Naples through a cable connection, radio waves or communication satellites. In Naples, the telephone exchange must connect your call to the phone you want to connect to. Each step is very fast, efficient and unnoticeable, and it is done million times a day.

All this process is maintained in function by teams of highly professional technicians and communication engineers. If you had been responsible functioning the public telephone network, you should surely have known more about transmission, signals, hardware commutators and other, but as a simple user you do not need to know all these details.

Fortunately, a computer local network is not as complicated as a international telephone one..

A computer network usually consists of:

1. connected calculation equipment (nodes):
   - server
   - work stations
2. Distributed equipment (resources)
3. Way of transmission (cables, radio waves, etc.)
4. Software that is used
5. Protocol that is used

Figure 10.1.1-1 Local Computer Network

10.1.2. Classification of Computer Networks

According to the covered geographical area, the networks are:

- local network (LAN): it connects several equipments withina building or institution. The maximum distance among such equipments should not exceed 1 km;
- metropolis network (MAN): it connects equipments and/or local networks that cover a locality. The maximum distance among such equipments may be of tens and even hundreds km;
- wide area network (WAN): it connects local or metropolis networks located in different area within a country or worldwide.

FIGURE 10.1.2-1

FIGURE 10.1.2-2

FIGURE 10.1.2-3

10.1.3. Computer Local Networks (LAN)

Local networks (LAN) are usually located in one building or in a campus with a surface of few km. They are normally used in order to connect personal computers of a company, factory, department or educational institution for allowing distributing the resources (printers, network disks, information and programs) and the exchange of information. Local networks are different from other types of networks by characteristics as: size, transmission technology and topology.
Local networks are of less size, and as a consequence, the transmission time can be easily forecast and there are no delays in data transmission. Thus, network administration is simplified.
The most common transmission technology is uses only one cable to which all equipments are connected. The function speed ranges between 10 and 100 Mbps (bps = bits/second), sometime even few hundreds within more modern networks; the delays in data transmissions are very small and only few errors occur.

10.1.4. Wide area computer networks (WAN)

WAN networks (Wide Area Network – wide-spread networks) interconnect LAN networks located faraway. WAN networks operate at 1 and 2 levels of OSI model (see In-depth analysis) and has the following characteristics:

- they operate on greater distances than LANs, this is why they usually use the services provided by ISP (Internet service provider). Such services can be bought or leased.
- They use serial connections. They generally provide a band width smaller than the LANs' one, and the its cost is also higher than the one for wide area networks.
- Wide area networks use a series of equipment that is adapted: routs (serial interface), WAN switches, modems, servers.

The routs (see 10.3.2) are te same ones that are used for the LAN connections, byt in this case serial interfaces are used, and such interfaces (usually) connect to a modem which transforms (modulates/de-modulates) signal type (electric/optical or copper cable /optical fiber) of the provider.
There are many WAN technologies which differ from each other by their distribution band width, data transmission way, price or reliability of the provided service.

WAN Technology

The transmission ways used for WAN networks are normally different from those used LAN networks.
WAN networks cover the long distance communication problems and the international borders ones as well; only financially powerful and big corporations can afford such private wide area networks. For the most of us, WAN means buying services provided by a communication provider. Such different choices include renting a telephone service public circuit, renting several communication services to a satellite connection or subscribing to a public network. Figure 10.1.4-1 illustrates a network including several types of LAN and WAN means.

FIGURE 10.1.4-1 *Network with LAN and WAN components.*

Compared to other LAN networks, WAN networks are relatively expensive. Usually, the cost depends on data transfer capacity the customer needs. Most services refers to choosing a certain specified capacity, which is charged for no matter if it is fully used or not. In case of WAN networks the customer does not need to think of the transmission mean; the provider is the one who provides it as well.
Compared to LAN networks, WAN ones offer lower performances, which are more expensive; working cost of a WAN network is directly connected to the traffic the WAN network is supposed to support.

10.1.5. Calculation Equipment Within a Network

Calculation equipment within a network can be:

- Server (offering services within a network)
- Work station (benefiting from the services provided by one ore more servers and having access to the distributed resources)
- Peer (working both as server and work station)

FIGURE 10.1.5-1 *Server* FIGURE 10.1.5-2 *Work Station*

According to their components, the networks can be:

1) Customer-server network

Separate Modem connected to a server

Separate printer connected to a server

server

Printer connected directly to a network

Customer 1 Customer 2 Customer 3

FIGURE 10.1.5-3 *Customer–server Network*

2) Peer-to-peer

FIGURE 10.1.5-4 *Peer-to-peer Network*

The difference between a peer-to-peer network and a network with a dedicated server is significant. Microsoft products support both types of networks, and the customer must choose according to his/her current needs.
The networks with centralized server are based on a highly specialized server. In most cases, the server is especially designed to provide fast and reliable services.

The information stocked on a centralized location can be easily protected. It is easier to maintain and manage the security system if the operating system (OS) is designed to provide a strict security and if the information was stocked in one location only.
Peer-to-peer networks allow each PC within a network to work both as a server and as a customer. Such network can provide high quality standard without using an expensive server, but it has a series of disadvantages:

2. The folders are dispersed on more than one work station, making harder saving security copies;
3. It is harder to maintain the security; Office PCs are barely as reliable as a centralized server;
4. You need a uninterruptible energy source (UPS) for you PC, so that you don't loose the information in you computer in case of an electricity break;
5. Peer-to-peer networks are very hard to manage. If the users use commonly the folders saved on their PCs, they shall keep a list of the members that may have access to the folders. Each PC has its own access control list. In case of new employees, the users must update the access control lists on their PCs (which supposes lost of changes).

In case the customer uses less important folders and services, he will be content with the peer-to-peer kind of network, but, if he/she uses the network for important activity, he/she should choose the server type.
Separated resources within a network refer to software and hardware components that can be separated within a network. Such resources are managed by a server, and they can be physically connected to it. Thus, there can be distributed resources connected to different workstations within a network, or even directly to the network.
Such distributed resources are: printers, hard-discs, modems, CD-ROMs, folders and directors.

10.1.6. Network Accounts

In order to efficiently manage the activity of a network and to provide its security, each user will receive an account characterized several rights to access the physical and logical resources of the network (folders, directors, programs, network drives, network printers), according to the user's needs and knowledge. Rigorous setting of the rights to access the network is critical for providing network's security; the network soft will support the compliance with the granted rights.
By Usual, these rights are set according to users groups with similar objectives. A group means several users having the same rights to access a certain network resource (for instance, you can define student groups, teachers and so on).
Creating work fields, of users groups and accounts with associated rights, as well as updating them is done by the network administrator, who is a high qualified person dealing with (installing) configuring and managing the network in order to provide efficient services and security.
Network security can be also be identified by the network administrator, who controls network resources, as well as the rights to access such resources.
Each network account will have an identification name – account name – and a password, which will protect the user's information. The password, formed of any printable characters, will have a length depending on the network operating system (of at least 5-8 characters). The users can change their password any time they consider it proper, during a work session, the password using the facilities provided by the operating system (for instance, security window options opened by Ctrl-Alt-Del during a Windows NT session or by set-pass command in Novell Netware).
Connecting to a network is the process by which the server managing the network is informed in case a user starts using the network's resources. The proceeding to logg off depends on the network operating system (for instance, logging window opened by pressing Ctrl-Alt Del in Windows NT, where the user should fill in his account name, the password and the domain he is logging on to or by login command in Novell Netware).

Logging off from the network is the process by which the server is noticed that the user stops using the network resources. After logging off the user can use only local resources of the computer (local hard-disk and the programs saved on the computer, floppy disks or CDs).

10.1.7. Distributing The Resources Within A Local Network

Within a local network several users can use in the same the physical or logical resources by using specific instruments provided by the operating system (for instance, in Windows NT, Share option in the contextual menu of the object). The distributed resources can be used by the users according to their access rights over such resources.

Physical resources distributed within a local network are the network disks and printers.

Distributed Drives within a network can be network disks or parts of disks (directors) – usually on the server computers. associating a logical drive name with a disk or a part of it is called mapping and it can be realized by a command specific to the network operating system. Thus, within a computer network, in the local drives list - A: floppy, C: local hard disk, ZIP unit or CD-ROM, etc., the user can add network drives, which refer to the disks on other network computers (usually, on the server). The users can distribute (or map) only the resources they have rights to access.

The printers connected to a network can be distributed for being available to more than one user. Network printers uses "a printing tale" which records the requests for being printed from several users, each user being able to command a series of “jobs" to be printed. Normally, the first job to be printed will be the first executed, and then the following an so on. (In the informatics terminology, a structure working using a principle according to which the first command is the first executed is called tale). If the some users have more important jobs to be printed then they take precedence, and the priority is changed.

For a user to be able to print using a network printer, it should be physically and logically installed – using a driver, be distributed and allow access to the user or the groups (groups) he/she belongs to. Managing the jobs to be printed using the network printers can be done (also) using special programs working according to customer-server principle controlling the printing processes (record them, allow the user to modify the parameters or even delete the jobs, etc.).

The access rights over the folders (including executable programs) and directors allows a proper use of distributed logical resources. Normally, such rights are granted by the network administrator according to users groups and they can be viewed (or even modified) by them (in Windows NT, the user can use Security option in the contextual menu, and in Novell Netware the user can use syscon utilities, rights and flag for viewing, or modifying the access rights over the folders). The most commonly used access rights within local networks locale are: Read (only read), Write, Change, Full Control (including the control over the access, changing the access rights over the resource).

10.1.8. Messages Within The Network

Any network operating system allows the users to communicate with each other by sending / receiving messages (in Novell Netware, the user can send messages by using the send command, but there are other options as well for sending messages, for instance, by using Norton Commander). Some utilities can even establish a dialog between users. The user can add to these facilities the E-mail system allowing the user to send longer messages, memorizing them, sending files, and this system should not be considered the same as the basic one.

A message can be sent to a user or to a group (on the same server or on other server). Receiving messages can be activated or deactivated by using the commands specific for the operating system.

10.2. Calculation Equipments Distributed Within Network

One of the main advantages of connecting to a network is the possibility of accessing by a user connected to the network the local equipments. Thus, at least theoretically, because there are no policies of restricting the access, all users within a network can have access to all others' resources. For security reasons, the users usually have access to the resources the owner allows them to use, but it still gives the users an unlimited number of possibilities. The second chapter of the module approaches the information regarding the categories of equipments distributed within a network , as well as physical elements for connecting making the connection possible.

10.2.1. The Server

The servers provide services within a network.
For a long time, the most common type of services provider within a network was the files server, although this kind of server was providing at least the following fundamental services:

- Jointly use of files
- Jointly use of network printers

Although there are several types of devices for distributing the printers, the network server remains the most efficient mean. Files services allow the computers within a network to use the files jointly with the other computers, transferring the files by network physical support.
Files services were also one of the main reasons for installing LAN networks. Before the LAN networks became accessible from the point of view of their cost, joint use of the files meant the transfer on physical support on which they were. Only few files could be modified on the floppy. Transferring a high number of files supposed using floppies with magnetic band.
Files services and printing services can be provided by using a special software on user's PC. Such software allows the users to jointly use the files on their hard-disks, as well as any printer connected to their PC. This approach is known as peer-to-peer network, due to the fact that all PCs within a network are considered equally important (see also 10.1.5).
A different approach uses a special server for providing files services and printing services. This server is usually called dedicated server, because it deals with providing files services and printing services exclusively.
In general, dedicated servers are based on a quite performing hardware, using Intel PCs of high speed or RISC systems. These systems must be fast, because they should meet the requests of many users at the same time. The dedicated servers have usually higher memory and capacity on their hard-disk units.
They also have characteristics improving their standard and their capacity. Their tolerance to defects allows the server to keep working even if one of their components is out of work. Supplementary disks mirroring tolerance defects in case of ordinary defects, when the primary disk has broken, the mirroring disk takes over its functions without interrupting the provided services.

Tolerant
to defects

High
Performance

FIGURE 10.2.1-1 A network starts with a server.

10.2.2. Categories Of Servers

Files services and printing services are not the only types of services a network can provide. There are many other kinds of communication servers:

- E-mail server. This type allows the users to exchange e-mail messages with other users in the same building or wide world.

- Modem server. This type allows the users t jointly use more than one modem, for calls within or outside the network. For such service it is not necessary that every person to have his/her own modem.
- Fax server. This type allows the users to send and receive faxes within a network. The users can receive faxes without having to print them. The faxes can be directed to the users similar to E-mails, without having to have a printed document.
- Portals. They aloe the users to communicate with mainframe systems or micro-computer or external networks as the Internet.

Figure 10.2.2-1 illustrates only few services a local network can provide for its users.

FIGURE 10.2.2-1 *A LAN network provides a wide services range.*

10.2.3. Operating Systems For Servers

A computer without an operating system (OS) is good of nothing. It is the operating system that gives the computer the possibility to communicate, stock information and run programs; it is the „heart" of the computer.

The servers use network operating systems. Having in view that they have to potentially serve tens or even hundreds of users, a files server or a printing one is usually a computer of high resistance. This is the reason a server needs an adequate operating system. A network operating system (NOS) must be powerful enough to simultaneously serve many users. A network operating system should also be reliable because many users count on it to accomplish their daily normal activities. We can notice that sometime we have to reinitialize the PC we are working with in case it does not respond anymore. What would happen if we have to reinitialize a network server serving hundreds of users?

Besides providing files services, printing services and others, a network operating system must be able to maintain network's security. LAN networks are more appreciated in business because they can provide more secure and cheaper services. But we have to notice that the managers do not want their unauthorized employees or the competitors to have access to some significant information. (in spite of the popularity of the hackers, most of the illegal action to gain access to electronic systems are from within the companies.)

FIGURE 10.2.3-1 *A network server needs a network operating system*

10.2.4. Workstations (Customers)

The customers use the services provided by the servers.

A customer is anyone who is a component of a network using the services provided by a server. The terms customer and server have their origin from a metaphor used in restaurant field (the servers provide „alimentation services" the customers of a restaurant derive advantage from). Due to the fact the networks are significantly based on the providers of services and customers, this type of network is also called customer-server network.

The most usual customers are the workstations of the users. Theoretically, any PC can be transformed into a network customer, and now many PCs are equipped by the manufacturers with Ethernet. All Macintosh computers are equipped for being connected to the network, as well as all Unix workstations. The manufacturers are now manufacturing computers so that they can be easily connected to the network the manufacturers are manufacturing now computers equipped for being easily connected to the network because more and more computers are sooner or later connected to a network.

Understanding the difference between the customer/server network and the old terminal/host networks, which were usually used for mainframe calculation systems, is critical. A terminal is a "bad" device „prost", without calculation facilities, in a terminal/host system; the terminal receives orders from the users and displays information for him/her, but all calculations are effected by the central mainframe system.

On the other hand a customer/server network, customer is a high quality computer himself. The customer can ask information from the server, but the customer computer makes most calculations. Although the customer uses the network for accessing the files, the printers and other common resources, he/she can execute very well most of the functions without needing a network.

The customer is usually wel individualized and configured for meeting the users' requests. Figure 10.2.4-1 illustrates an imaginary network consisting of a server and a customer.

Server   Customer (Workstation)

FIGURE 10.2.4-1 *Network with one server and one customer.*

10.2.5. Operating Systems For Workstations

Workstations use operating systems for workstations.

The workstations within an network (or customers) need de operating systems. The requests for a operating system designed for workstations are less stringent than those for a network operating system. Nevertheless, some of them have become so complex offering so many possibilities that they are almost as powerful as a network operating system.

The operating systems of the workstations have evolved and borrowed many characteristics of the network operating systems. In fact, it is possible to create complete networks only by using Windows for Workgroups, Windows NT workstations, Macintosh or Unix computers. But, in most cases, such networks are based on the joint use of the resources, so that a network operating system is still necessary.

FIGURE 10.2.5 -1 *A Server with several types of customers.*

10.2.6. Transmission Ways

For allowing the communication between the servers and the customers a "link"„ is necessary. This link is called transmission way.

Transmission way interconnects the servers and the customers and it is defined by a physical link through which the computers within a network can communicate with each other. The modality in which the connection to the transmission medium is realized, defines the physical topology of the network.

The range of the existent media is extremely wide:

- copper cable;
- optical fibre cable;
- radio waves;
- microwaves;
- infrareds;

PICTURE 10.2.6-1 *Network junctions, interconnected by transmission medium*

The majority of LAN networks use media made of copper cables or optical fibres. Copper is cheap and it is an excellent energy conductor, and the copper cables are by far the most popular choice for the LAN network medium. The performances of the copper cables have been improved year after year, until they enter in applications that other times were reserved only to the optical fibres.

However, the cost of the optical fibres has decreased and a large number of organizations which have avoided the optical fibres for a long time, now they are

choosing them because of their almost unlimited potential of performance. Although the performances of the copper cables continue to improve, the optical fibre will always be the ideal medium for the high speed networks.
The purpose of this section is that of presenting you the most utilized cables in the local networks.

10.2.7 The specific features of the transmission medium

A good choice of the transmission medium can be made, if some general medium features are taken into consideration. None of the medium excels in all of the examined features, and the decision should always take into consideration the medium which realizes the best compromise regarding the expressed requirements.
The specific features of the transmission medium are:

- The maximum distance between 2 network equipments without distorting the signal.
- The minimum distance minima between 2 network equipments.
- The maximum distance that can be covered by it.
- Sensitivity to electromagnetic interferences.
- Bandwidth.
- The cost with implementation.

Three of these features will be analyzed as it follows:

1. Sensitivity to electromagnetic interferences

The electrical signals and the magnetic fields are inseparable. The variation of the electrical signals from conductors creates magnetic fields around them, and the modification of the electric fields around the conductors creates electrical signals in the conductors. As a result, any source that produces variations of the magnetic fields can induce electric nature sounds in the network's cables. The LAN cables can also create magnetic fields that can interfere with the electronic devices from nearby, and with the electrical signals from the neighbouring wires.
The noise produced by the magnetic fields in cables is called electromagnetic interference (EMI). Some EMI sources of perturbation are: radio transmissions, electrical engines, fluorescent tubes or certain meteorological phenomena, like lightening. You have probably felt the effect of the electromagnetic interferences during telephone conversations.
Cables which are sensitive to the electromagnetic interference have still got a problem: all of them produce electromagnetic fields that interfere with radio signals. These radio signals are a security potential risk, because listening electronic equipment can receive the signals and, thus it can intercept the network transmissions.
If the security of the information used on the network is very important, there are two solutions for solving the problem. Optical fibres cables can be used, that, being not electrical, they can emit electrical signals or the signals used on the network can be coded.

6. Bandwidth

The bandwidth is a measure of the data transmission rates a certain medium can bear. Usually the cables used on the local networks can bear data transmission rates up to 20 megabits per second (Mbps). This limit for the transmission rate is sufficient for many local networks, but some of the new LAN services need higher speeds.
LAN networks are more and more used for the transfer of huge data volume – including large size files and audio, video or graphic data. These applications are extremely required, and a 20 Mbps bandwidth becomes insufficient when it is used by many network users at the same time. The network designers make considerable efforts in order to decrease the cost of the large band local networks, and now some network media can supply 100 Mbps bandwidths, with acceptable prices.

The bandwidth of a transmission medium can be used in two ways. When the whole bandwidth is allotted to a single data signal, the cable operates in *base band* mode. The majority of the LAN networks use base band signals.
When the bandwidth of a transmission medium is used for the transportation of many independent signals, the medium operates in *broadband* mode. You are accustomed to an example of broadband transmission through the cable that brings television signals to your home.
Thus, the programs of tens independent television channels can be watched. You can select a certain channel by using a remote control. The transmission medium operates alike, permitting a large bandwidth medium to transport much smaller bandwidth signals.

7. The cost

There are strategies for increasing the performance of a computer networks each on of them with its advantages and disadvantages. First of all, the cost of a network which assures the necessary speed for data transmission will be analyzed.
The speed is not the only factor that should be taken into consideration, when the cost is analyzed. Specially, in case of large LAN network dimensions, you must pay for facilities that make your network more reliable and easier to administrate. The administration of the network constituents' costs much more than the constituents themselves, but the supplementary cost is justified whether the bad function of the network is prevented from.

10.2.8 Coaxial cable

The coaxial cable is made up of two conductor wires that have a common axe. Two types of coaxial cables are met very often in cabling the local networks: the thick coaxial cable and the thin coaxial cable, preferred due to its ease of installing it and its lower cost.
Copper represents the more utilized medium in LAN networks, basically because of its lower prices. For a better understanding of how different types of cables are realized (coaxial, UTP, STP), we must understand what happens actually through the copper conductor.

Bits are coded as electrical signs. The easiest mode of coding bits might be the use of 0V (volts) for representing a logical "zero" logic and +5V for representing a logical "one". This procedure is called the NRZ coding (non-return to zero).
Moreover, for a better isolation of noise the electrical sign, a more complex method is used, namely the Manchester coding. In this coding, "1" is coded as a transition of the electrical sign from the small to the big, and "0" as a transition from the big to the small. The electrical noise may have a lot of causes, for example EMI (electromagnetic interference) and RFI (radio waves interference), and these ones are generated by electrical sources from nearby, as air conditioner or computers. These aspects have been taken into consideration when the coaxial cable was realized.

If the structure of a *coaxial cable* is examined, it can be seen its name comes from the fact that those two conductors – the central and the exterior screening conductor – have a common axe (see picture 10.1.15-1).

Isolation
Interweaved cover Dielectric Conductor

Father conductor type. BNC

PICTURE 10.2.8-1 The *structure of a coaxial cable*

The coaxial cable has a copper conductor, covered into a plastic isolator, which is also covered into a copper cover, assuring the protection to EMI and RFI. This cover is a part of the data circuit. All of these are introduced in an exterior cover that hinders the mechanic degradation of the wire. The wire ends with a BNC connector. Theoretically, it can be reached speeds of 10 - 100 Mbps (Megabits per second). Although, the signal is well protected by EMI, the coaxial cable has only a historical meaning in this moment, because it has been replaced with better alternatives, for example UTP and STP.

The coaxial cable components are as followed:

- The central conductor; in case of many coaxial cables, the central conductor is made up of a solid copper wire. The central conductors made up of interweaved wires can be used when the cables have to be flexible, but this conductor type reduces the cables' length that can be used. The solid conductors are preferable for permanent installations.
- Isolating layer. This layer serves for two purposes: from the electrical point of view it isolates the central conductor from the protection screen and it keeps it centered. To achieve the top of the performance, it should be physically maintained a constant distance between the central conductor and the protection screen.
- The protection screen. The protection screen is a conductor completely surrounding the central conductor. The screen serves as a second conductor of the cable and it protects the central conductor from the external electromagnetic interferences. The screening also reduces the electromagnetic signals emitted differently by the cable. For many years, the screening has been obligatory to the *LAN cables.*
- The cloak. A plastic or Teflon cloak protect the cable's exterior. The cloak isolates from the electrical point of view the protection screen from the outside and it protects it mechanically.

Picture 10.2.8-1 also presents a connector used usually together with the coaxial cable. This connector is called BNC connector (it comes from Bayo Net Connector), because it is installed by twisting it in the proper matched connector.

Coaxial cables have been used in the first LAN networks and they bear many characteristics that make them ideal for transmitting high speed data. The coaxial cable provides support for huge bandwidths, but most of the LAN implementations do not exploit this capacity.

The performances of the coaxial cable are strongly connected to its diameter and to the conductors' thickness. In order to improve the distance characteristics of the LAN networks with coaxial cables, the first designers have used thick coaxial cables, *which* were expensive, huge and hard to exploit. The recent projects have used thinner cables.

The coaxial cable types cannot be substituted between them. Besides the cable's diameter and the conductors' nature, another important characteristic of a coaxial cable is the *impedance.* The cable's impedance represents a measure of the total opposition of a cable resistance to current flow in an alternating current circuit, in this case under the form of data signals; the impedance is measured in *ohms.* The following network types need cables with certain impedance:

- RG-8 and RG-11 are coaxial cables of 50 ohms, with an approximately half inch diameter. These cables are used with the old Ethernet networks, usually called thick Ethernet or shorter thick net.
- RG-58 is a 50 ohms cable, thinner, used by an Ethernet standard usually called thin Ethernet or thin net. The RG-58 cable has an approximately quarter inch diameter and it is easier to use rather than RG-8 or RG-11 cables. However, a thicker cable can transport signals much farther.
- RG-59 is a 75 ohms cable; it is the same cable used in cable television networks. RG-59 cable is cheap and it is used for the implementation of a bandwidth Ethernet version.

The coaxial cables hold some advantages:

- The screening makes them more resistant to the electromagnetic interferences.

- The networks using the coaxial cable have been used for a long time (for 20 years in the case of the Ethernet networks), and that is why they are known, cheap and reliable.
- The coaxial cables are durable.

In spite of all this, the coaxial cables have also some disadvantages that should be taken into account:

- They are not totally invulnerable to the electromagnetic interferences and their use in areas where there is electrical nature sound should be avoided.
- They may be expensive enough – especially the thick coaxial cable types, which are closer to the optical fibre, from their price point of view.
- They are rigid – especially the thick coaxial cables.

The specialists recommend avoiding the use of coaxial cables for the newly designed networks.

10.2.9 Twisted Pair Cable (TP)

TP cable is made up of more isolated copper wires. The much more utilized TP cable type is the UTP cable (Unshielded Twisted Pair) used in telephony. The pairs of isolated copper wires are introduced into a plastic cover. The UTP cable is classified in many categories, in connecting the computer networks the 5th category cable being use. There is also the STP cable type (Shielded Twisted Pair) that holds a supplementary isolation layer, through inserting the pairs of wire into an isolating tube, which is introduced into a plastic cover.

10.2.10 The Shielded Twisted Pair (STP)

After the coaxial cable, the next type of cable used in LAN networks was the Shielded Twisted Pair - STP, presented in picture 10.2.10-1. Such a cable is made up of two isolated wires, twisted one around the other. Twisting the wires has not only the purpose of holding together the wires. As a result of the fact that the wires alternate their positions, the effect of the wires' electromagnetic interference is postponed. The twisting of the wires also reduces the cable's tendency to emit electrical signs; in the twisting absence, the two wires will tend to run as an antenna, taking the signals promptly from the outside, and emitting their own signals, which will lead to electromagnetic interferences in other devices.

PICTURE 10.2.10-1 *The Shielded Twisted Pair*

The cable presented in picture 10.2.10-1 is shielded for improving the cable's noise characteristics. As the screen of the coaxial cable, this takes the external signals that may cause interferences and it also takes the signals that would be emitted by the conductors on contrary.

The advantages of the shielded twisted pair:

- Resistance to electromagnetic interferences. The shielded twisted pair is practically insensitive to the electromagnetic interferences.
- Large bandwidth. Recently, to allow large bandwidths for the shielded twisted pair, the screening has been needed. 16 Mbps bandwidths have been reached since 1980.
- Durability. The shielded twisted pairs include huge weigh and robust conductors.

Disadvantages:

- Their cost is comparable to that of thin coaxial cables; however, generally, it is lower than the one of the optical fibres.
- The shielded twisted pairs can be rigid.

The shielded twisted pairs are still used, but, as the coaxial cables, they have become less popular. The shielded twisted pairs have fall into disfavor because of their high cost and their rigidity, which often affects the wires' route faster. Today, the accent is put on the unshielded twisted pairs.

10.2.11 The Unshielded Twisted Pair (UTP)

UTP (Unshielded Twisted Pair) is probably the most common cable used nowadays. The CAT1 UTP cable is a UTP cable type used in telephonic communications. The CAT5 UTP cable is used in networks and, at least theoretically, it can be reached a 100 Mbps speed. This cable contains four pairs of two wires, each one of them being covered into a plastic isolator coded to some colors and to the wires of each pair twisted around each other. All the conductors are positioned into an exterior cover, which assures protection against the mechanic deterioration.
The unshielded twisted pair (Unshielded Twisted Pair - UTP) uses twisted pair of wires, but it no longer has a screen. By eliminating the screen, the cost and the cable's rigidity are reduced, but it makes it more sensitive to electromagnetic interferences and it also increases the electrical noise, which the cable emits. The rigidity of the unshielded twisted pair is reduced because of the fact that many of such cables use relative small thickness wires – smaller than the ones usually used in coaxial cables and in the shielded twisted pairs. Picture 10.2.10-1 presents an example of UTP cable with two pairs of wires, and also the RJ-45 connector, which is usually used for this type of cable. The unshielded twisted pair has been firstly used in making the telephonic systems; actually, many of the connecting devices used in LAN networks made up with unshielded twisted pairs are borrowed from the telephonic system technology.

- Solid copper cable
RJ-45 modular connector

PICTURE 10.2.10-1 *The unshielded twisted pair with a RJ-45 connector*

Adapting the high level UTP cables for data transmission started in 1980. Some LAN networks types were introduced, but these were limited to relative small rates of data transmission. The original specifications of IBM for Token-Ring network limited the use of UTP cables for maximum 4 Mbps transmission rates, while the STP cables could be used up to 16 Mbps transmission rates (Token-Ring is a technology created by IBM, and IBM wrote the two words with capitals and introduced a hyphen between them. since Token-Ring is an IBM registered mark, other suppliers usually use lowercase. So, the lowercase will be used, when we do not want to mention the IBM Token-Ring product). In higher transmission rates, the cables tend to provoke electrical noise that can interfere with the cables or the electronic devices from nearby.

The clients' requirements regarding the higher transmission rates using the UTP cables made the producers to push up the limit referring to the maximum transmission rate; some networks may use the UTP cables at data rates up to 100 Mbps. however, to achieve these data transfer rates it was needed the defying of some classes of UTP cables with higher performances.
Here are the five classes or UTP cable types:
The 1st class. Cable class used only for vocal transmissions. They cannot be used for data transmission.
The 2nd class. Low speed data transmissions, such as alarm systems. They cannot be used for data transmission in LAN networks.
The 3rd class. Used for data transmissions with rates up to 16 Mbps. They are used for Ethernet UTP networks or token-ring.

The 4th class. Used for data transmissions with rates up to 20 Mbps. Generally, they are used in cases in which the 3rd type UTP cables are also used.
The 5th class. Used for data transmissions with rates up to 100 Mbps. Many of the new networks' projects with 100 Mbps transmission rates are based on this UTP cable type.
The unshielded twisted pairs are preferable, that are perceived as being more reasonable from their price point of view, than the shielded twisted pairs or the optical fibres. The 5th type UTP cables offer high speed, but there are also difficulties:

- The cable is more expensive.
- The connection devices are expensive.
- The cable workers have to be instructed more carefully.
- The installing procedure lasts longer.

As a result, the correct installation of the 5th type cables does not seem to be always a good deal. A seller estimates that the price difference between the 5th type UTP cable and the optical fibre is relatively small on working station (however, the electronic components needed for the optical fibre cable are considerably more expensive than the components used for the UTP cable).
Among the advantages of the unshielded twisted pairs are as followed:

- They are the cheapest cable types.
- the UTP cables have a reduced rigidity. Because many pairs of wire can be included in a single cable, a certain cable link can use several pairs of UTP cables than STP cables or coaxial cables.
- The installing methods are similar to the ones used in achieving the telephonic cables systems. The necessary tools are easy to obtain.

Among the important disadvantages are as followed:

- UTP cables are potentially very vulnerable to the electromagnetic interferences.
- Now, 100 Mbps represent almost the limit for the bandwidth of the UTP cables.
- Thin cables are the most vulnerable to the mechanical flaws.

10.2.12 The optical fibre

The cable from the optical fibre is a medium used for transmitting lighting signals. The technology used in achieving this type of cable has not been available until the 60's. The use of optical fibre cables provides many advantages. Firstly, they are not affected by electromagnetic interferences. Secondly, it can be reached faster speeds for data transmission. The speeds vary between 100 Mbps and 1Tbps (Terabits per second. Meaning, 1 followed by 12 zeros of bits transmitted in a second). These cables may have lengths between 2500 - 3000 m.

However, the price is still high, and a correct installation needs experience and specialized tools, the optical fibre is used due to the large distances it can cover and due to its characteristics: fast speeds of data transmission, reduced attenuation of the signal, unaffecting of electromagnetic interferences.

Optical fibre cables represent an almost perfect medium for transmitting data signals, and the new cable types promise to extend the limitation of the distances for allowing data transmission to thousands of kilometers. Unfortunately, the performances of the optical fibre cables are accompanied by a higher cost and few organizations permit themselves to use exclusively optical fibre cables.

Optical fibre cables have a glass or plastic core that transports data signals under the form of light impulses.
Picture 10.1.16-1 presents an example of optical fibre cable, as well as a usual connector for the optical fibre.

The cloak

Connector
Glass fibre or plastic material

PICTURE 10.2.12-1 *The optical fibre cable and a typical connector*

The optical fibre cables transmit lighting signals instead of electrical impulses. An "1" is represented by a stronger lighting signal, and a "0" by dark. These lighting signals are guided through the optical fibre cable. How? The conductor made of high quality glass and without impurities, with a big refraction index, called core. This is surrounded by a glass or plastic cover with a smaller refraction index, called cover. When the light passes through the centre it hits the edge, it reflects itself as in a mirror, thus remaining in the core. The centre and the edges are very delicate, and this is the reason for their covering into a material that assures the resistance and that it is covered itself into an external cover. The mechanical flows of the parts that direct lighting signals should be avoided. Even the smallest scratch of the centre will seriously affect the quality of the signal. This is one of the disadvantages of the optical fibre cable. The other one (and the most important one) is the price. The optical fibre is the most expensive medium of data transmission.

Because of the way in which some optical fibre cables are made, through them can pass much many lighting signals without interfering between them. This thing is possible by giving the lighting signals different angles in the cable input. This type of optical fibre cable is called *multimode*. The advantage is, of course, the price. It can be saved a lot when the multimode fibre is used, because fewer cables will be used. The disadvantage is that can have a maximum length of approximately 2500 m and it operates in lower speeds. The optical fibre cable that permits the passing of a single lighting signal only is called *single mode*. These cables are thinner and they may have a length of approximately 3000 m.

Because of the high speeds that can be obtained and because of the big amount of information, which are transmitted through this type of cable, the optical fibre is mainly used in buildings' interconnection (for example in a campus) or in the different building's floors.

But even the vacuum can be a medium for signals' transmission. Electromagnetic waves are propagated by air or vacuum at the light's speed. This characteristic made them ideal for applications as space ships, satellites or spatial wells, but also for earthly applications as, for example, the mobile phones.

10.2.13 The optical fibre cable components

Core. It is usually used the silicon glass, because of its higher transparence, but some plastic material core cables have been experimented, too. The glass cables can transport signals to many kilometers distances, without being necessary their refreshment, while the domain of using the core plastic cables is approximately of 100 de meters.

Isolating cover. An isolating cover surrounds the core. The characteristics of this cover are chosen carefully, so that the light is reflected back in the core, thus diminishing the signal attenuation.

Cloak . a hard cover, usually made of Kevlar, protects the cable. Many optical fibres can be put inside the same cable cloak.

The source of light for the optical fibre cable is usually a solid laser, called injection laser diode. (Injection Laser Diode - ILD).

The light made by the ILD laser has some useful characteristics. It is a monochromatic light, made of a single lighting wave length. Also, the light made by the laser is *coherent*, meaning that the all lighting waves are emitted in the same direction.

Although the optical fibre cable is not expensive comparing it with the copper cable, the reception and emission devices that are necessary are much more expensive than the equivalent devices used in copper cables.

The advantage of installing the optical fibre cable is the unlimited speed potential. Many organizations are forced to establish that the 100 Mbps bandwidth is insufficient. However there have been miracles regarding the increase of the UTP cables bandwidth, 100 Mbps seem to represent the speed limit for the unshielded twisted pairs. Although the copper cables function at a maximum traffic of 100 Mbps, the use of the optical fibre hardly starts. That is why, the use of optical fibres cabling represent an excellent choice in case of long term investments.
The optical fibre is superior to the copper cable for many points of view:

- The glass fibres are thinner and a large number of optical fibres can be put in an equal space with the one of a copper cable.
- Because for data transmissions light impulses are used, the optical fibres are immune in electromagnetic interferences, and they do not produce electrical noise. That is why, the optical fibre cables are the only LAN media virtual immune to the electronic spying.
- The optical fibre cables are durable. Glass cannot be degraded, and the connections are broken extremely rare.
- The optical fibre cables' bandwidth is unlimited for any use.

The cost of installing the optical fibre cables has constantly decreased, while better methods of installing have been improved. You can install optical fibre cables by using a bag of tools of some hundred dollars and after a couple of days training process. The reputation due to the installing high cost starts becoming obsolescent.

10.2.14 Other transmission media types

Radio waves

The speed of transmission by radio waves is situated in the 1 – 10 Mbps domain. The cost of an installing is average, and the medium is sensitive to interferences.

Microwaves

The speed of transmission is situated, as in the radio waves case, between 1 and 10 Mbps. The cost of an installing is proportional to the distance: low, for small distances and very high for large distances.

Infrareds

Locale networks are usually placed inside of a single building or group of buildings; however, the LAN networks may extend on some square kilometers surfaces. Because these networks include a large number of computers, often the transmission media are selected after the price criterion. The most used LAN networks transmission media are the copper cables, because they provide excellent performances at average prices. The optical fibres cabling may be used in such networks, especially in longer links and high speed connections. The optical fibre cables cost considerably more than the copper ones, and that is why, few companies use optical fibre for the users working stations.
We have to memorize that the most important characteristic of the LAN networks is the high performance at low prices.

10.2.15 The cable tester

If you want to make your own network cables, it is good to test them when you think everything is ready. This can be done in several ways. One of them is just to introduce the cable in NIC (Network Interface Card) and, if you are connected to the Internet, try to access a web page, for example http://www.google.com/.
If the plugs have been connected correctly, you will be able to visit the site.
And what happens if everything goes wrong? You would have no idea what was not working properly.

To discover the problems of a network cable, you should use a device called cable tester. There are some available on the market, with prices that vary between 100$ and some thousands dollars. Even the simplest cable tester can indicate the bad connections. The most sophisticated ones can give you details on the cable's length, can design maps of the wires, can test the level of noise made by the electromagnetic fields or they can help you find the cables in the walls.

Table 10.2.15-1 The characteristics of some cable types

Cable type	Bandwidth	Sensitivity to electromagnetic interferences	Cable's cost	Installing cost
Coaxial cable	Large	Low	Average	Average
Shielded twisted pair	Average	Low	Average	Average
Unshielded twisted pair	5-100 Mbps	The highest	The lowest	Low or average
Optical fibre	The largest	Insensitive	The higher	The higher

10.3. Network types

For a better understanding of how a network works, it is necessary to know which are the possible configurations, from the physical and logical point of view, in which can be connected several computers, so that it can be said that they form a network.
The chapter presents the main network categories, classified on their expanse and connections' type, as well as the used devices to extend the networks' dimension over the maximum length of the transmission medium.
The main logical topologies associated to a network are also presented.

10.3.1 Network topologies

Picture 10.3.1-1 Physical topologies

The topology defines the network structure.
The definition of the topology term contains two components: physical topology, the one that is given by the current configuration of the network cables and the logical topology that defines the mode in which the access is done. One of the most popular models of physical topology are those of the Bus, Ring, Star, Extended Star, Hierarchical and Mesh type (Picture 10.3.1-1).

- The Bus Topology:

It uses a single backbone cable segment, on which all the clients are directly connected.

- The Ring Topology:

It connects a host to the next one, and the last one again to the first one. This way, a cable ring is created.

- The Star Topology:

It connects all the cables to a central point of concentration. This is usually a hub or a switch.

- The Extended Star Topology:

It uses as a starting point the Star Topology. It connects the Star network types, by connecting the hubs or the switches. This way, the length and the network dimensions extend.

- Hierarchical Topology:

It is created similarly to the Extended Star, but, instead of connecting the hubs or the switches together (see 10.3.2), the system is tied to a computer that controls the traffic within topology.

- The Mesh Topology :

It is used in case no communication interruption is permitted (a military satellite's or a nuclear factory's command). Every host has its own link to the others. This mode actually reflects the Internet network project.

The logical topology of a network indicates the mode in which the hosts communicate through the transmission medium. The most used logical topologies are Broadcast and Token-passing.

- The Broadcast Topology means, that merely every host sends his own data to other network hosts. There is not a certain order used by the stations, it is worked after the first arrived principle, who is the first to be served. This is the mode in which the Ethernet network types work.
- The second type, token-passing, controls the access to the network by transmitting every host, sequentially, a token. When a host receives a token, this means that the host can send data to the network. If there is nothing to be sent, he gives the token to the next host and the process is resumed.

10.3.2. The network extension over the maximum length of the transmission medium

To extend the limit imposed by the transmission medium, special equipments are used, which are presented as followed:

1. Repeater

The Repeater is used in the imposed maximum limit overtaking of the cable's type or to interconnect the network segments based on different cables.

The Repeater is generally used in networks that use coaxial cable. Its role is to take over and to amplify the signal on a cable segment and to send it on the next segment. There are two important repeaters categories: some that send the received signal farther on and others that are capable to regenerate the signal, by eliminating the interferences.

The Repeaters can be also used for connection of the several cabling networks with different cables.

Further on, an example of using a repeater is presented, in a cabling network with thin coaxial cable.

PICTURE 10.3.2-1 *Repeater in a coaxial cable network*

2. Hub / Switch

The Hubs are used within the star topological network, which requires the existence of a central element the other entire network's components are connected in. A hub may be used to surpass the maximum limit imposed by the cable's type or to interconnect network segments based on different cables.

Generally, the hubs are used within the cabling networks with UTP cable. The physical topology of these networks needs a central element the other entire network's equipments are connected in. The Hub plays also the role of a repeater, because it transmits farther on the received signals.

A switch performs the same functions as a hub, at which is added the network data management.

PICTURE 10.3.2-2 *Hubs for 2 networks connection*

3. Bridge

The Bridge is a device used extending the maximum distance imposed by the transmission medium, but which accomplishes also the optimizing function of the network traffic, by the selective filtering of the sent data.
a bridge is capable of transmitting messages selectively only on segments that contain messages' addressees, thus reducing the network traffic, for a network made of several segments. Unlike a bridge, a repeater transmits signals farther on, no matter if the addressee is connected or not to that network segment. A bridge can be also used to interconnect two distinct local networks, which can be addressed as a single network.

10.3.3 The Token Ring Network

The Token Ring network (improved by IBM in the '70's) has a ring logical topology, but the wires are situated in star shape. Besides the fact that it guarantees to any network computer that it would be able to transmit data, its main advantage is that you can determine the minimum and the maximum waiting period until it is a computer's turn "to talk".
Imagine that you and your friends sit in a circle. One of you has a special object (the token). The one who has the token is the one who has the permission to talk; the others will listen to what the respective person talks about. A person may have the token for a limited period of time (so that everyone has the opportunity to talk). When the person who has the token has finished talking (or when his time is up) the token will be given to his right neighbour. This second person can talk now. If he has not anything to say, he gives the token to the next person from his right. Finally, the token will reach again the same person from who the "game" started and the sequence mentioned above is repeated endlessly.
Thus things occur in a token ring network. The Token is a sequence of 3 octets within token-ring. The most interesting part of a token is the octet of Access Control contained by it. This byte contains some important information used for the implementation of a priority system and of a management mechanism.
The priority system is used at the moment in which several stations need to access the network more often than the others. To each station is distributed a certain priority. Only the stations with an equal priority level or a bigger one than the level of the existent station in the token's priority field can obtain the token.
When a network device does not work anymore, some of the frames that have been sent can continue to circulate through the network for a long time, and there is the possibility of blocking the whole network. Fortunately, the token ring network management can identify this situation and can remove the network's error frames by generating a new token.

10.3.4 The FDDI network

FDDI means Fiber Distributed Data Interface and it is called to be an improved version of the Token Ring network. the FDDI network has a two rings logical topology. This means that it has been added a supplementary ring to improve the network's reliability. If one of the rings does not work anymore, the host will merely use the other ring. It is understood that in case the second ring does not work anymore, the network won't work either. Taking into consideration that the odds for the both of the rings not to work at the same time are smaller than a single ring's case, the FDDI network is reliable than the token-ring network. The FDDI networks are used in cases that the reliability and the necessity of determining the exact moment when it is a host's turn to transmit are extremely important, for example in the administrative building of a nuclear factory.
Besides the fact that the FDDI network cannot completely solve the reliability problem, there is also another disadvantage: the high cost. In these networks the optical fibre is used, and because there are two rings that need to be cabled, the price is relatively high.

FDDI Specifications

Speed	100 Mbps
The Maximum Cable Length	2000 m
The Coding	4B/5B
The Access Method	Token passing

There is also a cheaper option of the FDDI network: CDDI (Copper Distributed Data Interface) which, as it is suggested by its name, it use copper instead of the optical fibre.

10.3.5 Ethernet

At the beginning of the '60's the CSMA/CD basis were established (the protocol used by Ethernet) at the University of Hawaii, and in the '70's The Researching Centre of Xerox company in Palo Alto made the first prima Ethernet network. Since then, Ethernet became the most popular technology based on Layer 2 (see In-Depth-Analysis), because it is the most proper for the sporadic traffic network, but of fast speed of todays networks.
CSMA/CD is an abbreviation for **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection. But what does CSMA/CD actually mean?
Imagine that you went out for a movie with your friends and everybody wants to express himself about what he saw. If everyone spoke at the same time, no one would understand a thing. Instead, everyone expects to be quiet (this is the Carrier Sense part). If everybody is quiet, you take your chance and start talking. If two or many persons start talking at the same time, they will stop, and then, after a short time, they will try speaking again.
If two or many hosts start transmitting at the same time, it is said that a collision had taken place. When this thing occurs, the hosts that made the collision can detect it and they send a jamming sound so that every host should know what the situation is. After that, the stations that generated the collision do not transmit anything for a period of time chosen by chance; after this, they can start retransmitting. A special algorithm, known under the name of back-off algorithm is used to calculate this period of time. Finally, each station of the network will have the opportunity to transmit data, but, unlike the token-passing networks, the Ethernet is not deterministic (you cannot calculate how long a computer has to wait until it can transmit).
The Ethernet is a broadcasting network. This thing means that all the hosts from a network can see the frames of the junction that transmits, but only the host which has the MAC address that fits with the destination from the destination field will process the sending data. The rest of the hosts will ignore them.
There are over 18 types of Ethernet networks for which there are specifications or for which the specifications are still developing. In the table below, there are presented the most important.

The Popular Name	The Standard Name	The Speed	The Medium	The Maximum Length Segment
Orange Hose Ethernet *	10Base5	10 Mbps	Thick COAX	500m
Cheaper NET *	10Base2	10 Mbps	Thin COAX	185m
10 Base T	10BaseT	10 Mbps	Cat 5 UTP	100m
Fiber Ethernet	10BaseF	10 Mbps	Multimode Optical Fiber	2000 m
Fast Ethernet	100BaseT	100 Mbps	Cat 5 UTP	100m
Gigabit Ethernet over UTP **	1000BaseT	1000 Mbps	Cat 5 UTP	100m

* missed, ** ulterior development

10.3.6 LAN Media without Cables

Many people think that LAN networks should not use cables at all. Cables provoke disorder in offices and made the equipment's moving hard. Even if you haven't got any objection regarding the cables, you might come across situations when their installing is impossible, and as a consequence, several transmission media suppliers have tried to present on the market practical solutions of networks without cables.

Here are some of the situations in which the cables prove *to be undesirable:*

- If a network's data have to cross a street, you have two possibilities: borrow a telephonic line from a telephone service supplier (expensive) or use media without cables.
- If the users move frequently, the wireless transmission media will confer them a larger modality.
- If an organization modernizes and reorganizes frequently, the use of the wireless transmission media may be cheaper than the cables' periodical reorganization.

Now, when many persons from the different organizations' executive departments have portable computers, you may have a boss who, having the authority for asking this, will to move his computer form one place to another, without changing the cables' system.

There are available two types of wireless transmission media: the optical and radio media.

The LAN optical media use a similar technology to a modern TV remote control, between the devices infrared impulses are sent. The local optical networks operate mainly inside the buildings, but some types can broadcast between buildings situated at hundred meters.

The LAN radio media use a large diversity of radio techniques. Some of them use low power transmissions similar to the cell phones networks. Others have a high power transmission and they can transmit signals to considerable distances. Because the installing of high power transmissions, as the microwaves, needs licensed specialists, this section concentrates on the small distances transmission solutions.

10.3.7 The Local Optical Networks

The local optical networks can be implemented in two ways:

- By signal transmission to many receivers at the same time.
- By signal retransmission from a junction to another, using point-to-point transmissions.

Picture 10.3.7-1 presents a network that emits infrared signals in a room. The signals are emitted to a spotlighted surface situated on the ceiling, which distributes them to all the receivers from the room. This method does not claim precisely the alignment of the emitter and the receivers, as it is necessary in case of the point-to-point transmission solution. However, the receivers have to function in case of a lower level of lighting signals. That is why, this system can be sensitive at the excessive lightening of the ambient.

Picture 10.3.7-1 *The Operational Mode In Case Of A Local Optical Transmission Network*

The point-to-point transmission solution is presented in picture 10.3.7-2. Because a narrow fascicule is used, the receivers can function only with relative high level lighting signals. Of course, the emitter and the receiver have to be situated so that people walking through the office cannot obstruct them. This can be an important problem that has to be taken into consideration, towards the theoretical advantage of the wireless media – that referring to the ease in installing them.

Picture 10.3.7-2 *Point-To-Point Local Network*

10.3.8 Local Radio Networks

The majority of the wireless local networks use radio transmissions. Two technologies are available for the local networks:

• **Fn large band transmission** (spread spectmm). It is based on an army developed technology for sending the signals safely, extremely resistant to the noise.

• **18 GHz local networks** (18-GHz LANs). They use low power radio technology, similar to the cell phones networks.

10.3.9 Large Band Transmission

large band transmissions use more frequencies for transmitting a certain message. In one of the schemes, the emitter test different frequencies, by searching for the channel with the smallest noise at a given moment. The emitter indicates the receiver what the frequency he will use, so that the emitter and the receiver remain synchronized.

Another scheme divides the message in many parts, transmitting the different parts of the message on different frequencies. In order to make the data safer, on a separate channel fictive data can be sent. The legal receiver knows the frequencies that transport the real data, but the spies would have difficulties in remaking the original message from the many possible frequency channels.

The designers of the local large bands transmission networks have mainly used frequencies that do not require emission license.

The frequencies that do not require emission license can be freely used, the restriction being in a small number. Without the supplementary capacity given by the large band transmission technology, the use of unlicensed frequencies would be impossible.

large band transmissions can be strongly enough to pass through many wall types. That is why they represent a possible option in case of old buildings areas, in which cables cannot be installed.

10.3.10 18 GHz Local Networks

Motorola engineers have used their accumulated experience in the domain of cell phones in order to build a local network that operates similarly. The key of the cellular networks is represented by the use of low power radio transmissions, which cover a small domain, called *cell.*

The devices inside a cell communicate to a concentrator (hub) that functions as an emission-reception device for cell. In cases when a message is destined to an other device from the same cell with the message emitter, the concentrator retransmits the message to the cell. When a message is directed to a device situated in other cell, the concentrator sends the message through cable to the proper concentrator.

10.3.10-1 *Example of Motorola de 18 GHz Network*

It is noticed that the Motorola technology is not completely wireless. The computers communicate to the concentrators through the using modules, which are connected through cables. Also, many links from the concentrator to concentrator are made by cables.

10.3.11 Conclusions Regarding the Wireless Local Networks

The equipment suppliers for the local networks estimate often the expenses of moving the computers, in an organization's case, as having very high values. Their

purpose is to demonstrate that the supplementary wireless local network expenses do not compare with the necessary amounts in case of moving the computers.
These high expenses are hard to justify in reality. Within a modern cabling system, it is used to assemble cables in any place that is supposed a computer to be necessary. The moving of a computer is a simple thing, of unplugging the network, moving of the hardware in the new place and reattaching the computer to the network. The hardest work is the moving of the computer. The cabling of the system again, it will last only a few minutes.
Many wireless local networks are not really wireless ones. Cables for interconnecting the concentrators or to allow the devices to delimitate the interface modules with the network are necessary. Reorganizing the cabling of a „wireless" local network can be a major job.
The signals of the 18 GHz local radio networks, and the optical signals cannot pass through walls, and you have to use cables for one more time, in order to interconnect different sections of the local network.
The local wireless networks are surpassed from the performances point of view even by the lower performances cable networks. the Ethernet network supplies a bandwidth of 10 Mbps. The local wireless networks are rarely closer to the half of this value, and 6 bandwidth of 1-2 Mbps represents the usual value in their case.
Wireless LAN should be chosen only when the use of the cables is impossible. Some buildings do not allow the use of cables, from the structural point of view, and some organizations wish for their employees and computers to keep their mobility. Besides these requirements, it is difficult to imagine applications in which the wireless local networks represent the ideal technology.

10.4. Internet – General Presentation

In order to efficiently use a connection to the Internet, the user should have acknowledged the structure and the way an Internet network functions. For this purpose, we provide fundamentals regarding such network, describe the protocols, interfaces and the models being used, underlining the main services that can be used, describing them as well. Each element is approached herein related to the others for the user to understand its role and place per ensemble as shown in this networks network, the Internet. After attending this section, the user will know the fundamentals of the Internet network.

10.4.1 How and when the Internet network appeared?

The Internet, though it will be called this way only much later, starts in 1966 when the Advanced Research Projects Agency was founded (ARPA). The objective of this Agency was to create a main network for governing the USA army, which was supposed to stay operational even in case of nuclear attack. The Network's name was ARPAnet and it was operational in 1969, when it connected 4 personal computers in the university laboratories. The ARPA financed research projects initiated by American universities in network field, on the basis of which the Internet became to develop. The "practical" realization of such network was committed to BBN company. The sub-network was given IMP Honeywell DDP-316 minicomputers as routers modified, connected through telephone lines of 56 Kbps rented from several telephone companies. Each network node consisted in a host computer and an IMP (Interface Message Processors) located in the same room. For enhancing the security of the communication, each IMP was connected to other two. Initially, ARPAnet worked experimentally connected among four universities, and extended all over USA within only few years. In 1983, ARPAnet was divided into two distinct systems: MILNET (for military operations) and ARPAnet.

ARPAnet network proved the researchers its usefulness for fast communication among the research teams in different locations in USA, therefore, more universities wanted to connect themselves to it. The connecting procedures was restrictive due to the fact that ARPAnet network was financed by ARPA (briefly, by the Pentagon). By the end of the '70s, the National Science Foundation initiated a project for connecting the universities that hadn't had an agreement for cooperation with ARPA. At first, the agency offered e-mail services. In 1986 sub-network was created, connecting six super-computer centers in six American towns, each super-computer being connected to a LSI-11 (FUZZBALL) minicomputer, also called "the younger brother". Fuzzballs formed the sub-network to which they were connected into 20 regional networks. The network was called NSFNET.

In the mid '80s, the ARPAnet and NSFNET networks merged and, at the same time with the exponential increase of the requests for getting connected, everybody started to perceive this collection of networks as a huge networks connections. We can say that this is the moment the Internet network was born. It included in 1990, 3000 networks and 200 000 hosts. Today it is formed of over 100.000 LANs and millions of hosts. Such spectacular expansion of the network began in 1992, after voiding the interdiction to run commercial activity on the Internet and due to WWW services.

In relation with the Internet, there are two more terms that resemble, but having different meanings.

Intranet = local private network, based on the Internet applications and technologies. An Intranet belongs to a certain company and it is formed on physical and logical support of its local network. Thus, on the software applications necessary fir implementing a local network, software for creating, implementing and managing Internet services is implemented: internal site web, e-mail, groups of discussions, etc.

Extranet = an intranet for which the access was extended so that it can include legal and natural bodies from outside the company owing the intranet. An extranet can be designed for several purposes: for limited access of the customers, providers or co-operators; for on-line training; for electronic shopping services, etc.

10.4.2 Who manages the Internet network

Although the requests for managing such networks are countless, there is no supreme authority governing it. There is, though, a series of organizations working based on volunteers for investigating the problems that may occur and for submitting ideas for improvement.
Internet Architecture Board (IAB) is such an organization. Its members meet on a regular basis for debating subjects related to setting the standards, assigning the resources, trying to find long and mid term solutions. When a new standard is approved, it is published on the Internet, based on which new applications will be created, the purpose of which being a better compatibility between structures, operating systems, etc.
Another organization dealing with this issue is Internet Engineering Task Force (IETF). Its members meet on a regular basis for debating issues of short-term operational nature. When taking into account such issue, a work group is formed for exclusively researching that particular issue and finding the best adequate solutions. At the edning of such research, they have to draw up a report. According to its importance, it can become a source of information for anyone who's interested, can be accepted by anyone considering that it is a valuable solution or can be sent to IAB to be promulgated as a standard.

10.4.3 Who pays for the Internet network services

In opposition to was is expected, nobody "pays" for the Internet in ensemble and there is no Internet Inc. company, for instance, to cash the payments from all the Internet compound networks or its users. In exchange, everybody pays for his/her own connection. NSF pays for NSFNET, NASA for NASA Science Internet. A college or a corporation pays for its connection to a regional network, which in its turn pays a provider for its access to an international network.

10.4.4 What is the Internet for the individual user?

The fact that the Internet is not a computer network, but a collection of networks, is of no importance for the final user of the owned resources. For running a program or for accessing a certain data base the user does not need to know the way these networks interact. The only concern of the user is the problems that may occur.
Each network has its own operations center (NOC - Network Operation Center). Such networks discuss to each other and know how to solve their problems. The individual user has to contact the company providing access to the Internet. The company solves the problems or, in case solving the problem does not depend on it, it will hand it over to be solved.

10.4.5 How does the Internet network work?

Before you can fully understand the way you can adjust to the Internet, you have to understand the way to address to it. Everything you do on the Internet implies using an address associated to a computer within a network.
A computer address identifies it uniquely on the Internet and it is a succession of 4 natural numbers under 255, separated by "." (dot). Valid examples are: 141.85.255.96, 193.226.26.30, etc. We have to mention that the most significant numbers are those in the left side. The disadvantage of memorizing them by the user is obvious. This is why each computer in the Internet has its own special name. The basic restriction is that there should not be two computers in the Internet using the same name (IP address). The names are used only in order to make the using

of the Internet easier, the computers "preferring" to work with address in numerical format. The computers' numbers are stocked in data bases hierarchic distributed and organized. The system for transforming a name into an IP address and reverse is called DNS (Domain Name Service). There are only 7 distinct organizational domains as shown in the Table 10.4.5 - 1.

Table 10.4.5 - 1

Domain	**Use**
.com	Commercial organizations
.edu	Educational organizations
.gov	Non-military governmental institutions
.mil	Military organizations
.org	Other organizations
.net	Network resources
.int	International institutions (NATO)

Beside the organizational domain, there are some geographical ones. If the domain is outside USA, it will include a code indicating the country it belongs to. Each country has a code so that only by looking at a computer's name, we can find out where it is located. Some of more common codes are shown in the Table no. 10.4.5-2.

Table 10.4.5 - 2.

Domain	**Country**	**Domain**	**Country**
au	Australia	fr	France
ca	Canada	it	Italy
ch	Switzerland	pl	Poland
de	Germany	ru	Russian Federation
dk	Denmark	uk	Great Britain
es	Spain	us	United States

Remarks: The United States have their own geographical code. Though, within the Internet when no code is indicated, the user can assume the domain is located in the United States.

10.4.6 Recognizing someone's address

For becoming the addressee, each user of a computer connected to the network has added at the computer's address on which there is a name, which he/she and the administrator of the computer (for avoiding the situation when two users have the same name) chose (for instance, surname or name). Thus, for Cristian Doicin to receive an "e-mail", the address to send to will be "cristian.doicin@cont-edu.pub.ro". As you can in the example above, somebody's address can be obtained by adding the chosen name in the computer's address on which he/she can be accessed. Between the name and the computer's address will be the sign "@".

10.4.7 Recognizing a document's address

As it is shown in the section above, specifying the way in the director path of the computer can do finding a document on a computer. In the Internet network context, for finding a document, the user should add the computer's address the document was on. Moreover, due to the fact that on the Internet there are many kinds of services provided for the users, to the document's address, the user should add the path for obtaining the document. Generally, you can say that the document's address has the following general form:

service: address_server\path

The service can be:
http - "HyperText Transfer Protocol" – for reading the hipertext documents;
ftp - "File Transfer protocol" – for transferring a document.
Etc.
This address (service: address_server\path) is called URL ("Uniform Resource Locator").
The URL of a page consists in two components separated by // : the first part refers the protocol (http, ftp.), while the second one refers to the computer's address the resource we want to access is on. The address can be specified both through IP address and FQDN (Full Qualified Domain Name).
For instance: http://141.85.255.96 or http://www.yahoo.com. For navigating among the pages that have been already visited we do not need to tape pages' URL again, for it is enough to use the buttons Back and Forward.
URL can also contain other services as:
gopher - Gopher protocol
mailto – e-mail address of a person, with the general form: mailto:name@address_computer
news - Usenet news
telnet, rlogin and tn3270 – launching interactive sessions on other computers
wais - Wide Area Information Servers

10.4.8 The concept of Internet network architecture

the architecture of a network indicates the way the network's components interconnect, for achieving a certain way of functioning.
A system's architecture should provide information regarding the way the components of a system interconnect and regarding the interaction among them, but it also provides a general view of the system.
For reducing the complexity of its structure, most networks are organized on several layers (layers), in terms of strict distribution of tasks: each level is designed to provide certain services, on the basis of the services provided by the inferior layers. When two computers communicate, in fact, they realize a communication between the layers of the same rank of the two computers. N level of the A computer exchanges information with the n level of the B computer through a protocol called *n level protocol*.
In reality, the information is not transmitted from the n level of a computer to the analogue level of the other computer. As opposed to this, each level processes the information and transmits it to the inferior level, to the physical level where the effective exchange accomplishes. Only from the logical point of view we can call this a "conversation" between the levels of two computers. Between any of such adjacent levels there is an *interface*, setting the services to be provided for the superior level. When designing network architecture, the number of the levels and related interfaces must be clearly specified. The *architecture* of a network is formed of the large number of the protocols and levels.

10.4.9 What's a protocol?

A Protocol is an assemble of conventions and rules on the basis of which the user can send the information.
A computer network is made of a series of transmission means and calculation systems, for realizing both transport functions and functions for processing the information. A computer network interconnecting different calculation systems can work at their best only if there is a convention setting the transmission mean to transmit and interpret the information, this convention is called protocol.
An example can be the communication way between two philosophers, as shown in the picture.

Figure 10.4.9 - 1 – Communication way between two philosophers.

Two philosophers, in two different countries want to exchange ideas. Unfortunately, they are too far from each other and they do not speak the same language so that they could communicate.
In order to communicate, each philosopher hires a interpreter knowing bot languages, and each interpreter hires a secretary to send the message.
As shown in the picture, you can notice that the philosopher no. 1 sends the interpreter his message for the philosopher no. 2. The interpreter translates and gives it to the secretary to send it by fax, e-mail or the other secretary's phone.
We can notice in the previous example that for the communication to be achieved a lots of rules are necessary (protocols) which need to be set between the members of the same level and between the members within a group. This concept is called Protocols family (pile) and represents a list of protocols used by a certain system, a protocol for each level.
There are two types of protocols:

- routable: those protocols accepting LAN - LAN communication through several paths;
- non-routable.

Within the same group (philosopher – interpreter - secretary), among the participants to the communication, the exchange of information is based on other conventions, called services. Generally, the participants to the communication are called entities. These entities on an n level (for instance, the philosopher) provide a service used by n+1 level (in our case, the interpreter). N level is called services provider, and the n+1 level is called services user.

10.4.10 General Presentation Of OSI And TCP/IP Models

OSI Model - Open System Interconnection **–** is an interconnection model of open systems. The term "open" means that the system is able to be "open" for communication with any other system in the network if the system complies with the same rules (protocols).
ISO / OSI Model is structured on seven levels:
1. Physical level – for transmitting the bits through a communication channel;
2. Data connection level – for setting the bits transmission with no errors around a transmission line;
3. Network level – for controlling the way the sub-network works;
4. Transport level - its main duty is to accept data from its superior level (session level), to decompose them (fragment), if necessary, into smaller units, to transfer these units to its inferior level (network level) and make sure that all fragments are received correctly from the other end;
5. Session level – for managing the dialog between applications or users;
6. Presentation level – for the syntax and the semantics of the transmitted information among applications or users;
7. Application level – for the common interface for user applications, for transferring the files among programs.
OSI Model is just a network architecture model, because it indicates only what is supposed to do each level but it does not indicate the services and protocols used at each level.
OSI Model uses three essential concepts: protocols set between two entities at the same level, located in different systems; services set between successive level of the same system, and interfaces (interface of a level indicates to the next superior level how to make the access).
TCP / IP Model is older than the OSI model and it was used as a reference model by ARPAnet, and then by the Internet. The name of the model was given according to the fundamental protocols:

- TCP (Transmission Control Protocol)
- IP (Internet Protocol)

According to the following figure you can see the difference between the ISO / OSI reference model and TCP / IP model.

Figure 10.4.10 - 1 – Comparison between the ISO / OSI model and TCP / IP one.
There is just one mention about the network's host level made by the TCP / IP model, referring to the fact that the host should connect to the network in order to transmit information using a certain protocol. This protocol is not defined and varies from one host to another and from a network to another.
Internet level allows the hosts to emit package in any network and to make this packages circulate independently to their destination. Internet level officially defines a format of a package and a protocol called **IP - Internet Protocol** providing a transmission service of data with no connection necessary.
Transport level allows the communication between programs and applications. At this level two protocols are defined: **TCP - Transmission Control Protocol** is a point-to-point protocol, connection oriented which allow the octets flow sent from a system to reach any other inter-network system without errors.
The second protocol, **UDP - User Datagram Protocol** is an insecure one, without connections.
Application level allows the users of the network, through applications programs to use a variety of services.

10.5 Interconnecting the networks within the Internet

The Internet is o networks network. Within such network internationally spread one can find tens of thousands of local networks and wide spread networks. This chapter approaches the way the sub-networks the Internet is made of interconnect.

10.5.1 General Presentation

It is obvious that there are many kinds of networks, including LANs, MANs, WANs. Lots of protocols are used at each level. The existence of the networks of different kinds means, invariably, the need for different protocols.
It seems that all these kinds of networks (and implicit, of protocols) will co-exist for several reasons.
First, the number of such different installed networks is very high. Moreover, wireless communication is a very dynamic field with a lots of protocols continuously developing due to the new technologies, continuity issues and due to the fact that all manufacturers understood that their customers could easily change their services provider. Second, the cheaper the computers and the networks are, the lower the purchase level within an organization is. This can lead to installing UNIX workstations running TCP/IP in the engineering department and using Macintosh computers using AppleTalk in the marketing department.

Figure 10.5.1-1. Interconnected Networks Collection.
Third, different networks (for instance, ATM and wireless) are based on radically different technologies and due to the development of the hardware there always will be new and more adequate programs for the new hardware. For instance, the mid-range house today similar to the 10 years ago mid-range office; with lots of computers communicating to each other. In the future, it will probably be customary to connect the phone, the TV set and other appliances to a network in order to remotely control them.
To give an example of how one can connect all these to a different network, we can look at the situation illustrated in Fig. 10.5.1-1. We can see the network of a company with several head offices connected through a wide spread ATM. One of these head offices uses a FDDI optical backbone, connecting: a Ethernet network, a wireless LAN and a SNA computers network of the corporation's data center.
The purpose of interconnecting these networks is to allow the users in any networks to communicate to the users in other networks and also to allow the user regardless to the network he/she uses to access the information in any other network. For achieving this goal one should send the packages in a network to another. As the

networks often are essentially different, sending packages from one network to another is not always an easy task.
Regardless to the evolution of the IT world there will always be a variety of networks, which will have to interconnect to each other in order to communicate.
The connections can be of the following types:

- LAN-LAN: the user copies a files from another workgroup system;
- LAN-WAN: the user sends an e-mail to another user at distance;
- WAN-WAN: two users exchanging data;
- LAN-WAN-LAN: the users in different universities communicating to each other.

In order to physically two networks a "black box" should be placed at the junction between the two networks to be connected in order to solve the conversions necessary for the transmission of the data from one network to another. Such "black boxes" have different names depending on the level they work at, each of them being adequate for a particular interconnection type.

10.5.2 INterconnections being used

From the point of view of the functions of the OSI model at different levels we can highlight:
1. Repeater. It copies the individual bits between different cable segments, it does not interpret the intercepted packages and it represents the cheapest and easiest method of extending a local network.
Corresponding to the OSI model the repeater functions at the physical level, regenerating the received signal from a cable segment and transmitting it to another segment (figure 1).

FIGURE 10.5.2 - 1 – The Repeater according to the OSI model.

2. Bridge. It functions according to the principle that a network node has its own physical address. The bridge interconnects the LAN networks of the same type or different types.
The bridges are useful in case of the following situations:

- Physical extension of a LAN network;
- Interconnecting local networks using control techniques of the access to the different environments.

The bridges can be:

- Transparent bridges
- Bridges with routing through the source or Token Ring bridges.

If a company has several networks with different topologies, managing the flows of data can be done by a computer equipped with Ethernet as a bridge between these networks in order to correlate different physical networks in one logical network. All computers within this logical network have the same sub-network logical address.
3. Router. It functions at the network level of the OSI model and it is used for interconnecting several local networks of different types, using the same protocol of physical level.
The difference between a bridge and a router is that a bridge operates with physical addresses of the computers (from MAC), the routers use logical addresses of the computer.

FIGURE 10.5.2 - 2 Router in case of OSI model.

Generally, the router uses only one type of network level protocol and this is the reason it can interconnect exclusively the networks using the same kind of protocol. For instance, if there are two networks, the first using TCP/IP protocol and the second one IPX protocol, we will not be able to use a router using TCP/IP. This router is also called *protocol dependant router*. There are also routers with several protocols inserted, give user the possibility of routing between two networks using different protocols, called *multiprotocol* routers. A router is equipment combining the quality of a bridge and those of a repeater.

4. Gateway. The gateways allow the systems to communicate if their architectures are different and incompatible environments. A gateway connects two systems not using the same:

- Communication protocol;
- Formats structure;
- language;
- architecture.

The following connection can be done between the levels of the OSI model operating the equipment and its names:

- physical level - repeater, copies the individual bits between the different cable segments;
- data connection level – bridges interconnecting LAN networks of the same type or different types;
- network level – routers interconnecting several local networks of different types using the same physical level protocol
- transport level – gateways allowing the communication between different systems with different architectures and incompatible environments.

Lets take into consideration the situation as shown in the following figure. The source machine, *S,* intends to send a package to the destination machine, *D.* these machines are located in different networks, connected by a switcher. S embeds the package in a frame and sends it to its destination. The frame reaches the switcher, which determines, by analyzing MAC address, frame's destination, represented by LAN2. The switcher only takes over the frame from LAN1l and puts it on LAN2.

FIGURE 10.5.2 - 3 (a) Two Ethernet networks connected through a switcher,
(b) Two Ethernet networks connected through routers.

Lets reconsider the same situation having two Ethernet networks connected through a pair of routers instead of a switcher. A rent line of several kilometer lengths connects the routers. The frame is taken over by the router, and the package is taken from the data-base of the frame. The router examines the address in the package and it looks for it in its rout table. On this address basis it decides to send the package, possibly embedded in other kind frame according to the line's protocol. At the other end the package is put in the data field of an Ethernet frame and stocked on LAN 2.

The switchers do not have to understand the network level protocol, while the routers should be able to understand it.

10.5.3 What are the differences of the networks within the Internet

The networks can have a lot of differences compared to others. When the packages are sent from a source in a network they should pass through one or more foreign networks before reaching the destination network (which can also be different from the source one), a lost of problems may arise at the interfaces between networks. In the incipient stage, when the packages in a connection oriented network have to pass a network without connections, they may be reorganized. Such situation may be a surprise for the sender and an insurmountable problem for the recipent..

The difference between the maximum sizes of the packages used by different networks can create big troubles. How can a 8000 octets package can pass through a maximum 1500 octet size network? The differences between the quality of the provided services are a real problem when a package with delivery restraints in real time passes a network which is not able to provide any guarantee in terms of real time.

The control of the errors and of the flow is often miscellaneous between networks. If both the source and the destination wait for all the packages to be delivered in order with no errors but an intermediary network eliminates the packages each time it predicts a congestion, lots of the application will act unnaturally. The differences concerning the safety mechanisms, setting the parameters, the rules and even the national legislation regarding secrecy can also cause problems.

10.5.4 Virtual concatenate circuits

Two styles of networks concatenations are possible: a concatenation virtual circuits oriented and one with datagrams in the inter-network. In the past, most (public) networks were connection oriented. Then as the Internet started to develop, the datagrams became more into fashion. As the multimedia networks became more important, it is very likely that the orientation toward connection revive one way or another because it is much easier for them to guarantee the service quality with connections than without them.

FIGURE 10.5.4 - 1 Networks Interconnection using concatenate virtual circuits.
In the concatenate virtual circuits model a connection to a host in a network at distance is set in a similar way with the way the connections are normally set. The sub-network notices that the destination is at distance and builds a virtual circuit to the nearest router from the destination network. Then it builds a virtual circuit from that router to an external gateway (multi-protocol router). The gateway records that there is a virtual circuit with its tables and continues to build another virtual circuit to a router in the next sub-network. This process continues till the package reaches the destination host.
Once the data packages start circulate along the path, each gateway retransmits the packages making, if necessary, the conversion between the packages' formats and the virtual circuits number.
The scheme functions at its best parameters when all networks have the same properties.

10.5.5 Interconnecting the networks without connections

The alternative model of interconnection is the datagram model. In this model the only service the network level provides to the transport level is the capacity of injecting the datagrams în the sub-network. There is no guarantee that the packages reach their destination in their preset order if they reach they ever reaches their destination.
If each network has its own protocol of network level, it is not possible that a package in a network to pass another. The second problem, which is even more severe is the addressing. Lets take as an example a host in the Internet trying to send an IP package to a host in a network adjacent to SNA. The IP and SNA addresses are different.

FIGURE 10.5.5 - 1 Interconnection without connections
A better approach is to design an „inter-network" universal package and constrain all the routers to recognize it. Such approach is, in fact, the IP itself – a package designed to pass through several networks.

10.5.6 Passing through the tunnel

Solving the general case of interconnection of two different networks is a very difficult task. Nevertheless, there is an usual special case that can be managed. This is the case when the host and destination sources have the same network type, having a different network between them. Lets presume a multinational company with a TCP/IP network based on an Ethernet in Paris, TCP/IP network based on an Ethernet in London and a non-IP wide spread network (for instance, ATM).
The solution for such a problem is a technique called passing through the tunnels. For sending an IP package to host 2, host l builds the package containing the host's 2 IP address, inserts it in a Ethernet frame addressed to a multi-protocol router in Paris and then sends it to the Ethernet network. When the multi-protocol router receives the frame, it extracts the IP package, inserts it in the information field useful for the package of network WAN level, and addresses the package to the multi-protocol router in London, when it reaches this location, the router in London extracts tge IP package and sends it to host 2 within an Ethernet frame.

FIGURE 10.5.6 - 1 An automobile passing from France to England through a tunnel.
Using an analogy we can make the tunnels easier to understand. Lets imagine a person driving a car from France to England. In France, the car moves on the basis of its own power, but when it reaches the Canalul Mânecii, is loaded on a high speed train and transported to England through a tunnel. The car is in fact transported as the useful information. At the English end of this trip the car starts moving based on its own power again.

10.5.7 Routing within interconnected networks

Routing through a interconnected network is similar to routing within a sub-network. Lets presume the networks in the figure below, in which five net works are connected through six routers. Creting a graphic as a model of this situation is complicated because each router can access directly (meaning that it can send packages to) any other router which is connected to any network it is connected to. For instance, B in fig. 10.5.7-1(a) can directly access A and C through network 2 and D through network 3. This leads us to fig. 10.5.7-1(b).

FIGURE10.5.7-1 (a) A networks interconnection, (b) A graphic of networks interconnection.
Once the graphic was designed, one ca apply the regulation algorithms on the multi-protocol routers multitude.
An inter-networks typical package starts from its LAN addressed to the local multi-protocol router (in the MAC level header). After reaching this location, the code at the network level is te one deciding to what multiprotocol router to send the package, using its own regulation tables. If that router can reach its destination using the network protocol of the package, it is directly sent to that router. Thus, it is sent by using the tunnerl, embedded in the protocol required by the intermediary network. This process continues till the package reaches it destination network.

10.5.8 Fragmenting

Each network request a set maximum size for the packages to be sent. These limitations are the result of:
- the Hardware (for instance, the size of an Ethernet frame).
- The operation system (for instance, all tampon areas are of 512 octets).
- The protocols (for instance, the number of the bits in the lenghts field of the package).
- The conformity with some (inter)national standards.
- The wish of reducing at a certain level th retransmission caused by the errors.
- The wish of preventing blocking a tunnel with one package for a long time.

The trouble starts when a package has to pass a network the maximum size of which is less than the one of the package. To prevent such situation, we should try to avoid it, meaning by this that the inter-network should use routing algorithm, which avoids transmitting, the packages that cannot be handlded by those networks. What are the consequences in case the original source package is too big to be handled by its destination network? The routing algorithm is not able to avoid the destination and its only solution is to allow the gateways to part the packages into fragments, sending each package as a separate inter-network package.
There are two-oposed strategies for reconstructing the original package out of the fragments. The first is to make the transparent the fragmentation caused by the network with „small packages" for all successive networks the package passes through to its final destination (fig. 10.5.8 – 1 a). ATM Networks, for instance, have a special hardware to provide transparent fragmentation of the packages into cells and then reesembling them into the intial packages. In the ATM world, the fragmenting is called segmentation; the concept is the same one with only few differences.
The other strategy of fragmenting is that of not reassembling the fragments at the intermediary gateways. Once a package was fragmented, each segment is

considered an original one. All fragments pass a exit gateway (gateways) (fig. 10.5.8 – 1 b). Reassembling the parts into the whole is made only at the final destination host. This is the way the IP works.

FIGURE 10.5.8-1. (a) Transparent Fragmentation, (b) Non-Transparent Fragmentation

Non-transparent fragmentation also presents a series of problems. For instance, in this case each host need to reassemble the parts.

When a package is fragmented, the fragments must be counted so that it can be reassemble in the initial order. A method of numbering the fragments is based on a tree. If the package 0 (zero) need to be fragmented, the components will be named 0.0,0.1,0.2, etc.

A better numbering system uses the interconnection protocol of the networks to define a dimension of an elementary fragment small enough for the elelmentary fragment to pass through any network. When a package is fragmented, all its parts are equal to the elementary fragment, excepting the last one, which can be shorter. An inter-network package includes several fragments for a better efficiency. The inter-network header should provide the original number of the package and the number of the elementary fragment (or of the first fragment) included in the package.

This approach needs two sequence fields in the inter-network header: the number of the original package and the number of the fragment. There is a compromise between the elementary fragment size and the bits number of the fragment number. In such case, the extreme limit represented by an elementary fragment of one byte or octet, the number of the fragment being represented by the dee byte or octet in the original package (Fig. 10.5.8 – 2).

FIGURE 10.5.8-2. The fragmentation when the dimension of the elementary data is I octet, (a) the original package containing 10 data octets. (b) Fragments after passing through a network with a package's maximum dimension of 8 octets, (c) Fragments after passing through a 5 octet dimension gateway.

10.6 IP Protocol

The basic elements for a correct functioning of the network and the Internet are the protocols, the most important of which is the IP one (Internet Protocol). This chapter approaches the fundamentals of this protocol both in its initial version and in the one to be replaced with, the so-called IPv6.

10.6.1 Internet – network of networks

The Internet can be understood as a collection of sub-networks or **autonomous systems,** which are interconnected. There is no real structure but there are some major backbones. They are build up of high capacity lines and fast routers. The WAN and MAN networks are attached to these backbones, and the LANs in many universities, companies and Internet providers.

FIGURE 10.6.1 - 1 the Internet is a collection of many interconnected networks.

The bound which keeps the Internet together is the network level protocol, callaed **IP (Internet Protocol**). In comparison to the old network level protocols, this was designed from the very beginning in order to make possible the interconnection of the networks. Its task is to provide the best way (meaning, not guaranteed)to transport the datagrams from the destination source regardless to the location in the network of the machines involved or to the fact that there are other networks in between them.

The communication on the Internet can be as follows.

Transport level receives the data and fragments them into datagrams. Theoretically, the datagrams can be each of 64 KB, but, in practice, they do not exceed 1500 octets (for being able to fit in a Ehternet frame). Each datagram is transmitted through the Internet, fragmented in small units on its way. When all such units reach their destination, they are reassembled by the network level in the original datagram. The Datagram is then transmitted to the transport level, which inserts it in the entrance series of the receptor process.

10.6.2 IP Addresses

Each host and router in the Internet has its IP address, coding its network and host address. The combination is unique: there can be two machines with the same IP address. All IP addresses are of 32-byte length. An IP address actually does not refer to a host. It refers to a network interface. Consequently, if a host is located in two networks, it has to use two IP addresses. Though, in practice, most hosts are connected to only one network thus having only one IP address. For decades, IP addresses were divided into five categories as shown in fig. 10.6.2 - 1. This assigning model was called addresses classes. It is not *used* anymore*,* but the references to this model are common in the literature. Later, we will present the model replacing the address model.

FIGURE 10.6.2 - 1 IP addresses' format

A, B, C and D Classes format allow up to 128 networks with 16 millions hosts each, 16.384 networks with 64K host, 2 million networks (for instance, LANs) with 256 hosts each. It is also possible to send data-cast, the model directing each datagram to more than one host.

The addresses starting with 1111 are for later use. Over 500.000 networks are connected now to the Internet and their number is increasing each year. For avoiding conflicts, the network numbers are assigned by the ICANN (Internet Corporation for Assigned NAMES and Numbers). In its turn, ICANN assigned several local authorities to manage some of the addresses, and them in their turn, assigned the ISPs to other companies.

Network addresses, which are numbers of 32 bits, are usually written using the **period decimal system**. In this format each of the 4 octets is written in decimals from O to 255. For instance, the hexadecimal address C0290614 is written as 192.41.6.20. the lowest IP address is 0.0.0. and the highest is 255.255.255.255.

FIGURE 10.6.2 – 2 Network and Host Address

The values 0 and -1 have special meanings, as shown in the fig. 10.6.2 - 3. The Value 0 is the current network or the current host. Value -1 is used as an distribution address for assigning all the hosts in the indicated network.

FIGURE 10.6.2 – 3 Special IP Addresses

The hosts use the IP address 0.0.0.0 when they are started. The IP addresses with 0 as a network number refers to the current network. These addresses allows the computers to refer to their own network without knowing the number of the network (but they have to know the address class in order to know the number of how many zeros they need). The addresses consisting exclusively of 1s allow the distribution in the current network, usually a LAN. The addresses with an exact network number and exclusively 1s in the host field allow the machines to send packages in LANs at distance, anywhere in the Internet (although lots of system administrators disable this option). At last, all the address of the 127.xx.yy.zz type are reserved for loop-back tests. The packages sent to this address are sent wirelessly; they are locally processed and considered received packages. This allows sending packages to the local network without the sender having to know its number.

10.6.3 Sub-networks

All the hosts in a network should have same network number. This characteristic of IP addressing can lead to some problems when the network extends. Thus, lets presume an university that at first used a B class network for the computers in the Ethernet network of the Computers Department. A year later, the Electric Engineering departments whishes to have access to the Internet, so it buys a

repeater for extending de computers Department's Ethernet in their building. In time, many other departments have purchased computers and the limit of four repeaters per Ethernet is fastly reached. Now another system is necessary.
Purchasing another network address would have been difficult because there are not enough addresses and the university had already had addresses for over 60,000 stations. The problems becomes a rule regarding the fact that one A, B or C class address refers to only one network, not to a multitude of networks. As more and more companies face this kind of problem the addressing system has been modified in order to solve it.
The solution would be allowing a network to be divided into several parts for internal use, functioning as a whole, only one network, for the external one. Nowadays, a typical campus network can be as shown in the fig. 10.6.3 - 1, with a main router connected to an ISP or to an WAN and lots of Ethernet networks all over the campus in different departments. Each Ethernet has its own router connected to the main router (possibly through a backbone LAN)

FIGURE 10.6.3 - 1. A campus network consisting of several LANs in several departments
According to the literature, these parts are called **sub-networks.** Using the word with such meaning creates a conflict with the „sub-network" term, which refers to the *totality of all routers and communication lines in a network*. Fortunately, the meaning of the word can be understood from the context it is being used.
When a package reaches the main router, how does the router know to what sub-network (Ethernet) to send? The existence of a table with 65,536 records in the main router could be the answer. Such records would indicate it what router to use for each station in the campus. But for this a very large table would be necessary to enter so many information in the main router and a lot of manual work each time a new station would be added, moved or eliminated.
Fortunately, there is another solution. Instead of using only one B class address with 14 bits for the network number and 16 bits for the host, a number of the host's bits are used for creating a sub-network number. For instance, if an university has 35 departments, it could use 6 bits of the sub-network and 0 bits of the host. This would allow using 64 bits of the Ethernet networks, each of them with maximum 1022 hosts (as we have already mentioned, 0 and -1 are not available).
For using the sub-networks, the main router needs a **sub-network mask**, indicating the separation between the network number, sub-network and the host, as it is shown in the fig. 10.6.3 - 2. The sub-network masks are described in the same decimal system by adding a "/" (slash) followed by the number of bits from the network + sub-network. From the example illustrated in the fig. 10.6.3 - 2, the sub-network mask can be described as 255.255.255.0. An alternative system is /*22* for indicating the fact that the sub-network mask is 22 bit long.

FIGURE 10.6.3. – 2 A B class network divided into 64 sub-networks
Outside the network, the division into sub-networks is not obvious. In this example, the first sub-network can use IP addresses starting from 130.50.4.1, the second can start from 130.50.8.1, and the third can start from 130.50.12.1 and so on.

Sub-network l: 10000010	00110010	000001|00	00000001
Sub-network 2: 10000010	00110010	000010|00	00000001
Sub-network 3: 10000010	00110010	000011|00	00000001

In this example, the vertical bar (|) shows the limit between the sub-network number and the host's number, in the left side I one can find sub-network 6 bits, in the right side – host's 10 bits.

10.6.4 Routing without classes among domains

IP is intensely used for the last few decades. It has been functioning extremely well as it was proved by the exponential development of the Internet. Unfortunately, the IP becomes the victim of it own popularity: it peters out its addresses. This disaster has generated lots of disputes and controversies in the Internet world.

In 1987, some visionaries predicted that one day the Internet would increase by 100.000 networks. Most experts stated that this would happen in decades, if ever. The 100.000th network was already connected 1996. Theoretically, there are over 2 billion addresses, but the way they are organized by classes millions of these are wasted. In particular, the guilt ones are the B class addresses. For most of the organizations, an A class address, with 16 millions of addresses would be too large and a C class network, with 256 address would be too little. A B class network, with 65536 addresses is the best choice.
When these three classes were created, the Internet was a research network connecting the most important USA universities (plus a small number of companies and military sites doing research in this field). By that time, someone stated that: „The USA has approximately 2000 universities and colleges. In spite the fact all of them are connected to the Internet and many more other foreign universities connect to the Internet, we will never reach 16.000 because there aren't so many universities in the whole world. Moreover, the fact that the hosts is a whole number of octets fastens the speed of processing the packages."
Though, if 20 network bits had been assigned for the B class networks, another problem would have appeared an explosion of the routing tables. From the point of view of the routers, IP addresses space a hierarchy on two levels with network numbers and hosts numbers. The routers don't need to know all the hosts, but it has to learn about all networks. If half a million C class network had been used, each router in the entire Internet would have needed a table of half million entries, one for each network, indicating which line is used for getting to a particular network together with other information.
The solution that has been implemented giving the Internet a little bit more space is CIDR (Classless InterDomain Routing). The main idea of CIDR is to assign IP addresses, which remained as blocks of different dimension regardless to the class they belong to. If a site needs, lets say 2ock 000 addresses, it is given a 2048 address block at a boundary of 2048 octets.
Eliminating the classes makes the routing more complicated. With CIDR, there is only one routing table for all networks, consisting in on vector de triplets (IP address, sub-network mask, exit). When a IP package arrives, the first thing to do is extracting the destination IP address. Then (conceptually) the routing table is scanned entry by entry, masking the destination address and comparing it to the table entry, looking for a match. It is possible that more than one entry (with sub-network masks of different length) to match, in case the longest mask was used. Thus, if there is a match with a /20 mask and a /24 mask, the /24 one will be used.
Lets take into consideration the case in which million of addresses are available starting with 194.24.0.0. Lets presume that South-Bank University needs 2048 addresses and it was assigned with the addresses from 194.24.0.0 to 194.24.7.255, with the mask 255.255.248.0. Then, Oxford university asks for 4096 addresses. Due to the fact that a 4096 addresses block must be lined up at a 4096 octet border, these cannot be numbered starting with 194.8.0.0. on the other hand, addresses from 194.24.16.0 to 194.24.31.255 with 255.255.240.0 mask are assigned. Cambridge University asks for 1024 addresses and it receives addresses starting from 194.24.8.0 to 194.24.11.255 and 255.255.252.0. mask.
The assignments are illustrated in the Tab. 10.6.4 – 1
Tab. 10.6.4 - 1.

University	First Address	Last Address	Number of Addresses	System
South-Bank	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Cambridge	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
Available	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

Routing table from all over the world are no updated with the three assigned entries. Each entry contains a basic address and a sub-network mask. There are enough information to send the package on the right line.

10.6.5 Translating the network addresses

IP addresses are sufficient. An ISP could have a /16 address (former B class) assigning 65.534 station numbers. More customers than this number can be a problem. For the home users with dial-up connections the solution is to dynamically assign and IP address to each computer when dials and renounce it when the session ends. This way one /16 address can be used for 65.534 active users, which probably is sufficient for an ISP with several hundred thousands users. When ending the session, the IP address is reassigned to another computer that is dialing.
Although this kind of strategy works well for an ISP with a moderate number of home users, it doesn't really work for the ISPs providing services for companies. A company needs to be continuously connected on-line during working hours. this is the reason why each computer needs to be associated with it own IP all day long. In fact, the total number of the computers of the companies that are ISP's customers cannot be higher than the IP addresses owned by it.
The situation is even more serious. More and more users subscribe from home at ADSL and cable Internet. Two of the services provided are (1) the user receives a permanent IP address and (2) there is no connection tax (only a monthly tax), this is why many users of ADSL and the cable Internet stay permanently connected.
He situation is even more complicated, many users of the ADSL and the cable Internet have two or even more computers at home, some time one for each family member and all of them want to be on-line using the only IP address that was assigned to them by the ISP. The solution is to connect all their computers through a LAN and put them on a router. From the ISP's point of view, the family is now a company owing few computers.
The problem of using all IP addresses is not a theoretical one. It is a real and actual one. A long-term solution is that all Internet to migrate to IPv6, which address is of 128 bits. The process of adopting the new system is developing slowly and many years will pass before it will be achieved. The short-term solution is NAT (Network Address Translation).
The basic concept of NAT is to assign to each company one IP address (or at least less addresses) for the Internet traffic. Within the company, each computer will receive an unique IP address, to be used for the internal traffic. When a package leaves the company and goes to the ISP, an address translation is made.

Fig. 10.6.5 - 1 Placing a NAT unit and its way of functioning
Within a company each machine has its unique 10.x.y.z address. When a package leaves the company it passes through a NAT box (NAT box) converting the internal IP address, 10.0.0.1, see the figure, to the real IP address of the company, here – *198.60.42.12,*. NAT unit is often combined in a device with only one firewall, providing security by carefully controlling everything that goes out and in the company.
There is a problem though: when the answer comes (for instance from a Web server), is addressed 198.60.42.12, so how can the NAT unit know which address to replace it with? *That* is NAT's problem. If there had been a free field in the IP header, that field could have been used for memorizing the real sender, but only 1 bit hasn't been used.
What happened next? The NAT designers have noticed that most IP packages had TCP or UDP content. They both have headers containing a source port and a destination one. These fields provide the field necessary for NAT to work.
NAT is only a temporary solution. The real solution would be the implementation of IPv6.

10.6.6 IPv6

IP (IPv4) in its current form is already out of date. If in the beginning the Internet was used mostly by the universities, the top industry and the USA government (mostly by the Defense department), once the interest towards the Internet rose, starting with the mid 90s, the Internet started to be used by different catega început să fie utiliies

of people. On one hand, lots of people having laptops use it in order to keep in touch with the base at home. On the other hand, at the same time with the imminent convergence of computers, communication and entertainment industry, it is very likely that in the nearest future any phone or tv set becomes an Internet node producing a billion of machines used for audio or video on order.
Knowing these problems, in 1990 IETF started to work on creating a new IP version, one that would never use up all addresses, and be able to solve a large range of other problems being more efficient and more flexible.
The major objectives were:

- To maintain billions of hosts, even with inefficient assignment of the address space.
- To reduce the size of the routing tables.
- To simplify the protocol in order to allow the routers to process the packages faster.
- To provide a higher security (identification and confidentiality) compared to the current IP.
- To pay more attention to the service type, especially for the data in real time.
- To help the multiple sending allowing the domains to be specified.
- To create proper conditions for a host to migrate without having to change it address.
- To allow the protocol to develop in the future.
- To allow the co-existence of the new and the old protocol for few years.

Up to December 1992, seven serious and interesting propositions were submitted for discussions. They varied from barely modifying the IP to eliminating it completely and replacing it with a brand new protocol.
Three of them, the best of them, were published in *IEEE Network*. After a lost of discussions, revisions and reviews, a combined version was chosen, called by then SIPP (**Sin Internet Protocol Plus**) and it was recalled Ipv6.
IPv6 achieves its task worthwhile. It uses the good characteristics of the IP, eliminates or diminishes the bad ones and adds some new ones and it is necessary to do so. Generally, IPv6 is not compatible with IPv4, but it is compatible with the other auxiliary Internet protocols
In the first and most important place, IPv6 has longer addresses than IPv4. They are 16 octet long, solving the problem IPv6 was created for: to provide a unlimited source of Internet addresses.
Another really important improvement of IPv6 is that it simplifies the header. It contains only seven fields (compared to 13 in IPv4). This change allows the routers to process the packages faster, thus improving the productivity and diminishing the delays.
The third improvement is a better support for options. Moreover, the way the options are represented is different helping the routers to avoid the options that do not concern them. This characteristic fastens the processing of the packages.
A fourth characteristic the IPv6 for improving the system is that it provides a higher security.
At the end, the new model pays more attention to the quality of the services.

10.6.7 Mobile IP

Many Internet users have portable computers and they want to stay connected to the Internet when the visit an Internet site at distance and even in between these two. Unfortunately, the IP addressing system makes this easy to say.
Each IP address contains a network number and a host number. For instance, lets presume a machine with the IP address 160.80.40.20/16. 160.80 part indicates the network number (8272 in decimal system). All routers in the whole world have routing tables indicating which line to be used to get to 160.80 network. Any time a package comes with the 160.80.xxx.yyy destination IP address, the package goes using that line.
If the machine with that particular address is transferred into another place in the Internet, the packages will continue to be routed to the home LAN (or the router).

The owner will stop receiving its mail and so on. Assigning a new IP address to the machine, an address corresponding to its new location, is not a good choice because a lot of persons, programs and databases would have to be notified of such change.
Another way of approaching this situation is that the routers do the routing using the complete IP address instead of exclusively using the network address. In spite of all this, such strategy would lead to a situation in which each router would request millions of table entries for an extremely high cost for the Internet.
The solution is detailed below. Each site wants to allow the users to relocate and for this it has to provide a local agent. Each site that wants give the users access has to create an agent for the foreigners. When a mobile host goes into a foreign site it contacts the foreign host there and it registered itself. The foreign host then contacts the local agent of the user and gives it **the intermediary's address**, normally, agent's own IP address.
When a package reaches user's residence LAN it goes to a router that is attached to the LAN. Then the router tries to find the host in an usual way, by distributing a ARP package asking, for instance: „What's the Ethernet address of 160.80.40.20?". the local agent answer to this question giving its own Ethernet address. Then the router sends the packages for 160.80.40.20 to the local agent. The agent, sends them through the tunnel to the intermediary's address by embedding them in the field of the useful information of a IP package addressed to the agent for the foreigners. Afte this, the agent for the foreigners unpacks them and delivers them to the mobile host's address.
There nothing to impede the project accept that a mobile host be its own agnet for foreigners, but this approach is valid only if the mobile host (as the agent for the foreigners) is logically connected to its current site in the Internet. It also has to be able to get a (temporary) address that can be used by the intermediary. That IP address must be of the LAN it is currently attached to.
How to find the agents? The solution would be that each agent to regularly distribute the address and the service type to be provided (for instance, local agent, for foreigner, or both). When a mobile host reaches a place, it can listen waiting for such distribution to the so-called **announcements**.
Another problem is the security. When a local agent receives a message kindly requesting him to re-send all the Cristina's packages to an IP address, before re-sending them, it should first check if the request really comes from Cristina or from somebody else trying to impersonate her. For this purpose identification cryptographic protocols are used.

10.6.8 Controversies over adopting IPv6

We have already mentioned the dispute over the length of the address. The result was a compromise: addresses of a steady 16-octet length.
Another issues under controversy refers to the length of the field *Jumps' limit.* The answer was that each field can be enlarged thus leading to a disproportionate header. The function of the *Jump's Limit* field is to impede the packages to wonder for a ling time and 65.536 jumps are too much. At last, the more the Internet develops, the more distance links will be created, and getting from one country to another will be made in at most half a dozen jumps. If a package needs more than 125 jumps to get from the source or destination to their international gateways their national backbones are definitely not working properly. Those supporting the thoery of the 8 bits has won the battle.
Another puzzling question refers to the maximum size of the package. The community of the supercomputers wanted packages larger than 64 KB. When a supercomputer starts sending information, it is a serious problem and it does not want to be interrupted after each 64KB. The argument against the larger packages is that in case a 1 MB package reaches a T1 line of de 1,5 Mbps, that package will monopolize the line for over 5 seconds causing a significant delay for the interactive users using the line. The answer was also a compromise: normal packages were

limited to 64 KB, and the jump-by-jump extension header can be used for the larger packages.
Another important issue is eliminating the IPv4 control sum. Some stated that this is similar to eliminating car's breaks. By doing this, the car becomes lighter and, consequently, faster, but in case of something unexpected it can face serious problems.
The argument against the control sum is that any application taking care of the information integrity has to have a control sum at the transport level, so that maintaining another IP sum is an excess. Moreover, the experience indicates that in IPv4 calculating the IP control sum is very expensive. IPv6 has no control sum.
The mobile hosts were also under dispute. If a portable computer passes through half the world is it possible to continue operating at the destination the same IPv6 address or should it use a diagram of the local agents or agents for the foreigners?
The mobile hosts introduce asymmetry in the routing system. It is possible that a small portable computer to hear a strong signal sent by a stationary router, but stationary router will not be able to hear the weak signal sent by the mobile host. Consequently, some people wanted to include in IPv6 an explicit support explicit for the mobile hosts. Such effort failed because there was reached no consensus regarding a proper proposition.
But the most disputed problem was the security.
An aspect of this disputes referred to where to locate the security for many countries (not all of them) has a very severe export legislation regarding the cryptography. Some of them, for instance, France or Iraq, strongly reduce internal using of cryptography, so that no one can hide any secrets from the police. As a result, any implementation of an IP using a encrypting system strong enough to be of a real value cannot be exported from the USA (and many other countries) to the customers all over the world. The need of maintaining two program sets – one for internal use, the other for export – is an issue the computer companies don't agree with.
An issue that everyone agreed with refers to the fact that no one expects that the Internet based on IPv4 be closed Sunday morning and the next day be replaced by the Internet based on Ipv6. Some "islands" will be converted step by step by the IPv6, initially communicating through the tunnel. By the time the IPv6 islands develop, they will fusion into larger islands. In the end, all islands will fusion and the Internet will be completely converted. Due to the massive investment into IPv4 routers currently in use, the conversion process will take at least a decade.

10.7 TCP/IP diagram's protocol

This chapter briefly approaches the main protocols specific to the reference model TCP/IP.

10.7.1 General Presentation

The following diagram described below is called *protocol graphic* and it illustrates some of the most common protocol specific to the *TCP/IP* reference model.

- FTP Protocol (File Transport Protocol)
- HTTP Protocol (Hypertext Transfer Protocol)
- SMTP Protocol (Simple Mail Transport Protocol)
- DNS Protocol (Domain Name Service)
- TFTP Protocol (Trivial File Transport Protocol)

The TCP/IP model allows maximum flexibility for developing the applications (at the application level).
The transport level allows two protocols - transmission control protocol (TCP) and user datagram protocol (UDP).

10.7.2 File Transfer Protocol - FTP

The files are transferred through this protocol between the machines using it. It has in fact a dual structure, both protocol and program. As a protocol, FTP meets the

requirements of the applications, and as a program it used for manually operating the files.
FTP makes the connection transparent due to its Telnet technology with FTP server, and then created the support for operating the files, for instance, listing them, handling the folders, viewing the transfer of the files between the stations.
For limiting the access, a process of identification is necessary when accessing a FTP server, adding to this process a password. Most FTP servers also allow anonymous access (without password), but the options in this case are limited.

10.7.3 HTTP Protocol (Hypertext Transfer Protocol)

This is the acronym for HyperText Transfer Protocol. This protocol sets the rules of the hypermedia files' transfer. The applications using this protocol – the two partners at the ends of the connection – are considered abstract entities from the point of view of the protocol. These entities have to be able to make requests and/or receive answers (customer-server model). One of the basic concept - taken over by other protocols – is the resource one, a computer, a database, a document, a service in general. The resource has to be able to be referred to correctly and unequivocally. For the resource's reference in the Internet it is used the generic name of URI - Uniform Resource Identifier, which is able to identify a location, such identifier being called URL - Universal Resource Locator or a name , such identifier being called URN - Universal Resource Name. The protocol the paradigm is based on is the request/answer one. The customer asks for the access to a resource, the resource is identified by the URI, and the servers answers by a state line. The simplest situation is the one the connection customer-server is made through one connection. In general, there are many intermediaries along a connection.
There are three types of intermediaries:

- proxy – is a sophisticated intermediary: receives the requests sent to a identified resource by URI, rewrite some parts of the message and then sends the request to the initial server. The proxy server can make some checking (identification, security, and so on) which are difficult to implement to all the machines that are connected to that proxy. The proxy server should be considered as a representative of a whole group of customers, negotiating their requests addressed to "the rest of the world".
- gateway – is a intermediary similar to a proxy one, but from the point of view of a server. It is similar to a waiting room located in front of a server or of a group of servers. The servers that are "behind the gateway" are not visible, they being represented by the gateway. The requests received at the gateway are routed to the server that is able to answer it, or to the freest server available that can answer it in order to efficiently use the calculation power. *The gateway* also makes a protocol conversion, thus, the server will not have to "recognize", the "http" protocol.
- tunnel – is an unintelligent intermediary: it transports information it doesn't understand or interpret in any way from one connection to another. At one end of the tunnel there usually is a gateway server, and at the other end is a proxy one.

A proxy can work with several customers at the same time being able to filter the received requests.
Addressing a resource can be done using the constructions of the following type:

http://address_host [:portal] /path/subpath1/.../subpath_n/name_document

where:

- http- the name of the protocol being used
- address_host identifies a server or a gateway in the network, using usual DNS address
- :portal specifies the information portal to connect to, implicitly :80
- /path/subpath1/.../subpath_n/ - the absolute path to the document name_document on that particular server

Remarks: the reference resource is not necessary an entire document, it can be just a part of the document.
The server answering the requests regarding hypermedia documents is called server WWW and "knows" the http protocol.

10.7.4 Trivial Files Transfer Protocol (TFTP)

This type of protocol can be considered as the FTP's „younger brother", making all the files transfer, bu in this case, the user need to know exactly what he/she is looking for and where to look for the needed information, TFTP being able to exclusively receive files. It does have so many functions as FTP, but opens exclusively the public files and it has to implement no identification system, which makes it less secure, this being the reason it can be used in very few cases.

10.7.5 Simple Mail Transfer Protocol - SMTP

Sending mails (letters) was one of the first services provided to the users of a network and it is having a really tremendous success. Nowadays, the e-mail is a very fast method of sending information and communicating, being cheaper even than the traditional mail. There were created a lot of "discussion lists" where the participants can discuss the issues they are interested in. There are often moderators supervising the discussions and verifying the compliance with the set rules for the list (there are rules regarding the "behaviour" which shouldn't be disobeyed; one of the most important rules is behaving civilized without using insults or trivial language; of course, for being accepted in some "discussion forums", being rude is a basic condition...). The user have to comply with some rules regarding the behavior, which form the so-called NETiquette.
In order to send a message the user should run a specialized program (there is the PINE program in Linux). Each network should have an e-mail server. The rules for sending messages from one e-mail server to another have been set in the SMTP protocol (*Simple Mail Transfer Protocol*).
Probably the most used protocol, this sends and receives information as e-mail messages format. It uses an algorithm called „spooling". In fact, SMTP inserts the information to be sent in the messages' tail and then sends it. When receiving a message, it is stocked on a device, usually a disk, and the destination network's server periodically checks this disk and sends it to the destination station.

10.7.6 Transmission Control Protocol - TCP

This protocol finds and corrects the errors occurring during the transmission. The TCP on the sending device will make a connection to the receiving device, and they negotiate the information quantity to be sent, this ensemble being known as „virtual circuit". This type of communication is called „connection-oriented communication". TCP is a very steady and precise connection counting the received segments and correcting the errors. It takes over the information blocks, which it divides into segments, this segments being then numbered. At the destination, the TCP protocol there is able to re-assemble the received information from the sender. After sending each sequence (numbered segment), the TCP protocol sending the information will wait for the receiving confirmation from the receptor, and in case it doesn't it re-send the segment.

Using the TCP is necessary only in case the fiability is veru strict, this protocol usually significantly delaying the data transmission. For a faster transmission and less strict one the user should use a UDP protocol.

10.7.7 User Datagram Protocol – UDP

similar to the TCP, this protocol is used to send segments, but in UDP case, the transmission applies to those segments which don't require a very exact control.

Very often, using the TCP makes a network designed to be faster acts like a very slow one, because of the delays coused by the opening, maintaining and closing a TCP connection. UDP is much faster, and this is obvious from the way it functions.
Similar to the TCP, the UDP segments the data and attaches a number to each segment, with the difference that it does not turn the data into sequences and is not interested in finding out the way they reach their destination. The UDP has no confirmation, receiving or sending mechanism during the transfer, it just adds numbers to the segments and work continuously, similar to the way Tcry P does. After sendin the messages, the UDP forgets about them, le completely abandons them. The UDP is not a connection-oriented protocol, it does not create a virtual circuit and it does not contact the destination.

10.7.8 Internet Protocol - IP

The protocol was approached already in a previous section. As it is mostly used for the Internet, it identifies different network devices finding out the network they are on and the elements describing the devices.

FIGURA 10.7.8 – 1 TCP/IP Protocol Diagram